Vaaratiedottamisen tekninen kehitys

Mikko Lammi

Tampereen yliopisto
Informaatiotieteiden yksikkö
Tietojenkäsittelyoppi
Pro gradu -tutkielma
Ohjaaja: Erkki Mäkinen
Syyskuu 2014

Tampereen yliopisto
Informaatiotieteiden yksikkö
Tietojenkäsittelyoppi
Mikko Lammi: Vaaratiedottamisen tekninen kehitys
Pro gradu -tutkielma, 90 sivua, 1 liitesivu
Syyskuu 2014

Vaaratiedottamisen tarkoituksena on varoittaa ja opastaa välittömässä hengenvaarassa olevia ihmisiä yllättävissä ja laajoissa vaaratilanteissa. Perinteisesti tähän on Suomessa käytetty väestöhälyttimiä ja joukkotiedotusvälineiden kautta välitettyjä vaaratiedotteita. Mobiiliteknologia tarjoaa kuitenkin uusia menetelmiä välittää sekä nopeammin että kohdistetummin varoituksia uhattuina oleville henkilöille. Vaaratiedotteiden jakelua olisi myös mahdollista tehostaa erilaisilla Internetin jakelukanavilla, kuten sosiaalisen median palveluissa.

Tutkimuksen tavoitteena on selvittää, millaisia nykyaikaista viestintä- ja tietoteknologiaa hyödyntäviä vaaratiedotejärjestelmiä maailmalla on käytössä ja suunnitteilla, ja pohtia, miten nämä soveltuisivat käyttöön Suomessa parantamaan olemassa olevia varoitusjärjestelmiä. Käyn läpi matkaviestinverkkojen teknologiaa sekä paikantamisen että kohdistettujen massaviestien näkökulmasta, sekä esittelen keinoja, joilla Internet-viestinnässä voidaan tavoittaa paremmin kansalaisia ja varautua yllättäviin kuormitusongelmiin. Työssä luodaan myös katsaus 2000-luvulla Suomessa tehtyihin viranomaisselvityksiin ja lakihankkeisiin vaaratiedottamisen modernisoimisesta.

Lisäksi hahmottelen erään mahdollisen korkean tason arkkitehtuuritoteutuksen monikanavaiselle vaaratiedotteiden välitysjärjestelmälle ja esittelen tapoja arvioida tällaisen järjestelmän toteutuksen arkkitehtuurisia ratkaisuja.

Avainsanat: viranomaiset, vaaratiedote, pelastustoimi, matkaviestinverkot, paikannus, sosiaalinen media

Alkusanat

Tutkimuksen aihevalinnan pääasiallisena motivaattorina on ollut halu saattaa oma ammatillinen asiantuntemus mobiiliverkoista riittävälle tasolle niin nykyisten verkkojen kuin tulevien uusien teknologioidenkin osalta. Toinen yhtä merkittävä syy on ollut viranomaistiedottamiseen liittyvät kysymykset kansalaisen näkökulmasta – monien muiden tapaan olen ihmetellyt, miksi kohdennettuja vaaratiedotteita ei ole käytössä, vaikka tarvittava tekniikka on ilmeisesti ollut olemassa jo pitkään.

Tutkielman kirjoittaminen päätoimisen työssäkäynnin ohella on valitettavasti vaikuttanut sen kestoon. Aloitin kirjoittamisen loppuvuodesta 2011, jolloin aiheesta ei juurikaan ollut kotimaista tutkimusta saatavilla. Sellaista alkoi ilmaantua vasta vuosien 2013 ja 2014 aikana Jyväskylän yliopistosta, Pelastusopistosta ja Poliisiammattikorkeakoulusta. Vaikka nämä hankkeeet ovatkin osittain oman työni kanssa päällekkäisiä, on ne tehty julkaisuunsa saakka täysin toisistaan tietämättä. Havaitsin ilokseni kuitenkin myös muiden päätyneen moniin samansuuntaisiin päätelmiin kuin omakin tutkielmani. Myös asiaan liittyvä lainsäädäntöprosessi on edennyt. Kesällä 2012 eduskunta hyväksyi uuden lain vaaratiedotteista. Tämä ei kuitenkaan ottanut kantaa vaaratiedottamisen teknisiin menetelmiin, joiden osalta tutkielmassa esitetyt kysymykset ja ratkaisuehdotukset ovat edelleen ajankohtaisia.

Tutkielman tekeminen on osoittanut yllättävän kiinnostavaksi projektiksi, mikä luontaisen tiedonjanoni tuntien ei ole ollut sinällään yllätys. Koenkin arvokkaaksi, että varsinaisen opinnäytetyön ohella olen tutustunut myös laajaalaisesti niin yhteiskunnan toimintaan (pelastustoimi ja varautuminen, lainsäädännön ja julkisten hankkeiden prosessit), teknologiaan (paikannus ja mobiliteetin hallinta matkaviestinverkoissa ym.) sekä tieteellisiin tutkimusmenetelmiin. Ainakin tämän työn kohdalla matka on ollut antoisampi kuin pelkkä päämäärä.

Haluan kiittää seuraavia yrityksiä mahdollisuuksista päästä vuosien varrella kurkistamaan mitä erinäisimpien mobiiliverkkojen ja tietojärjestelmien konepellin alle (sekä osallistumaan niiden toteutukseen): Accenture Oy, CGI Suomi Oy (ent. Logica Suomi Oy), Comptel Oyj, CSC Oy, DNA Oyj, Elisa Oyj, EADS Secure Networks, EXFO (ent. NetHawk Oyj), TeliaSonera Oyj, Seven Networks International Oy, Conmio Oy sekä Upcloud Oy.

Espoossa, 28. elokuuta 2014
Mikko Lammi

Sisällys

Käytetyt lyhenteet ja termit

2G	Toisen sukupolven matkaviestinjärjestelmät (GSM)
3GPP	3rd Generation Partnership Project
3G	Kolmannen sukupolven matkaviestintäjärjestelmät (UMTS)
4G	Neljännen sukupolven matkaviestintäjärjestelmät (LTE)
ATAM	Architecture Tradeoff Analysis Method
BSC	Base Station Controller, tukiasemaohjain
BTS	Base Transceiver Station, tukiasema
CAP	Common Alerting Protocol
CBS	Cell Broadcast System
ETSI	European Telecommunications Standards Institute
GGSN	Gateway GPRS Support Node
GMLC	Gateway Mobile Location Center
GPRS	General Packet Radio Service
HLR	Home Location Register
HTTP	HyperText Transport Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPAWS	Integrated Public Alert & Warning System
JMS	Java Message Service
LA	Location Area
LBS	Location-based Services, paikkaperusteiset palvelut
LCS	Location Services
LVM	Liikenne- ja viestintäministeriö
MSC	Mobile Switching Center, matkapuhelinkeskus
MSISDN	Mobile Subscriber International Subscriber Directory Number, matkapuhelinnumero
SGSN	Serving GPRS Support Node
SM	Sisäministeriö
SMSC	Short Message Switching Center, tekstiviestikeskus
SS7	Signalling System No. 7
TMSI	Temporary Mobile Subscriber Identity
UM	Ulkoasiainministeriö
VLR	Visitor Location Register
WEA	Wireless Emergency Alerts
WWW	World Wide Web

1. Johdanto

"Mikä on punainen ja kovaääninen, joka auttaa ja ärsyttää?"
[Harju, 2009]

1.1. Miksi televisio piippaa, mutta puhelin ei?

Tapaninpäivänä 26.12.2004, noin klo 8 paikallista aikaa, tapahtui Sumatran luoteispuolella voimakas maanjäristys, joka aiheutti laajan hyökyaallon eli tsunamin ympäri Intian valtamerta. Hyökyaalto osui varoittamatta noin klo 10 aamulla pohjoismaisten turistien suosimalle Thaimaan länsirannikolle aiheuttaen mittavaa tuhoa alueen infrastruktuurille. Kuolonuhrien määrä pelkästään Thaimaassa nousi lopulta useisiin tuhansiin. Onnettomuuden aikaan alueella oli noin 3000 suomalaista matkailijaa. Etenkin katastrofin alkuhetkillä tiedonkulku Suomeen oli varsin hidasta ja viranomaisten tiedotus kangerteli niin tuhoalueella oleville kuin heidän omaisilleenkin kotimaassa. Kun pääministeri ilmoitti televisiossa Poliisin julkaisevan verkkosivuillaan listan kadonneista, tukkeutuivat sivut välittömästi, kun tuhannet omaiset ja vielä lukuisammat uteliaat yrittivät turhaan päästä näkemään listaa.

Tiedonkulkua hankaloitti huomattavasti viestintäverkkojen ylikuormittuminen tuhoalueella. Nopeasti havaittiin, että tekstiviestit menivät paremmin läpi kuin puhelut ja näistä muodostuikin tärkeä viestintätapa alueella oleville. Ulkoasianministeriö sai lopulta 29.12. teleyritysten avustuksella lähetettyä massatekstiviestinä evakuointitiedotteen yli kuuteen tuhanteen Thaimaahan paikallistettuun suomalaiseen matkapuhelinliittymään. Viesti saapui varsin myöhään, eikä se lopulta merkittävästi vaikuttanut evakuointien onnistumiseen [OTK, 2005]. Kadonneista omaisistaan tietoa etsivät puolestaan löysivät epäviralliset, vapaaehtoisesti kootut nimilistat Thaimaassa sukelluspalvelua tarjoavan suomalaistaustaisen yrityksen verkkosivuilta. Se vaikutti kestävän kuormitusta huomattavasti poliisin sivuja paremmin.

Onnettomuuden jälkipuinnissa mediassa sekä viranomaisten selvityksissä perättiin osana viranomaisten kriisiviestinnän parantamista mahdollisuutta tekstiviestitiedottamiseen laajemminkin vaaratilanteiden yhteydessä. Viestintäviraston *viestintäverkkojen tekniset viranomaisvaatimukset* -työryhmän raportissa [Viestintävirasto, 2005] luonnosteltiin teknistä ratkaisua alueellisesti kohdennettujen hätätekstiviestin lähettämiseen ja arvioitiin järjestelmän käyttöönottokustannuksiksi noin 1,5 miljoonaa euroa. Tämän jälkeen asia kuitenkin hautautui viranomaisselvityksiin, joissa asian etenemistä hidastivat niin lainsäädännön muutokset kuin Hätäkeskuslaitoksen uudistaminenkin. Kustannusten maksajaa palloteltiin eri ministeriöiden välillä.

Järjestelmän tarve nousi esiin julkisessa keskustelussa aina erilaisten suuronnettomuuksien ja muiden laaja-alaisten vaaratilanteiden yhteydessä. Konkreettisin hyöty siitä olisi epäilemättä saatu Nokian vesikriisin yhteydessä marraskuussa 2007, kun merkittävä osa kunnan vesijohtoverkosta saastui [Seeck *et al.,* 2008]. Tekstiviestitiedottamista olisi pystytty käyttämään ilman tilaajien paikantamista, sillä vastaanottajat olisi voitu valita liittymän haltijan kotiosoitteen perusteella saastuneen vedenjakelun alueelta. Tätäkään mahdollisuutta ei käytetty. Syksyllä 2009 LVM:n alainen VIRVA-työryhmä julkisti lopultakin esityksensä ministeriölle, että tämä tekisi päätöksen viranomaisten ja teleoperaattoreiden yhteisen kohdennettujen viranomaistiedotteiden välitysjärjestelmän rakentamisesta [VIRVA, 2009]. Hätätiedote oli kuitenkin muuttunut ”*muuksi viranomaistiedotteeksi*”, koska viestinvälitysteknologiassa nähtiin jopa useiden tuntien viive, joka olisi hätätiedotteille liian pitkä. Raportissa arvioitiin, että järjestelmä saataisiin käyttöön puolessa vuodessa päätöksestä. Asia ei kuitenkaan edennyt niin nopeasti, vaikka ministeriön turvallisuusjohtaja Rauli Parmes olikin jatkuvasti tiedotusvälineiden haastatteluissa toiveikas järjestelmän käyttöön saannista. Vuosi VIRVAn raportin jälkeen hän arvioi Helsingin Sanomissa, että valmius viesteihin olisi saatu vuoden 2011 kesään mennessä. Toisaalta samaan aikaan oli vielä ratkaisematta järjestelmän lopullinen tekninen toteutus ja ennen kaikkea maksaja [Palttala, 2010]. Tätä tutkielmaa kirjoittaessa kesällä 2014 tekstiviestitiedotteita ei ole edelleenkään otettu käyttöön.

Televisioon hätätiedotteet tulivat Suomessa vuonna 2009. Lähetyksiin ilmestyi ruudun yläreunassa juokseva punainen teksti huomioäänimerkin saattelemana. Tämä olikin huomattava parannus aiempaan tilanteeseen, jossa tiedotteet välitettiin ensisijaisesti vain radion ja teksti-TV:n kautta. Järjestelmä kuitenkin sai nopeasti kritiikkiä osakseen useistakin syistä. Kaikki hätätiedotteet näkyivät koko maassa, tiedotteet olivat vain suomeksi, ja hieman yllättäen ne aiheuttivat uusia ongelmia: uteliaat kansalaiset lähtivät etsimään tiedotteissa varoitettua asuinalueella liikkuvaa karhua sen varomisen sijaan. Poliisi sai myös vastaanottaa vihaista palautetta MM-jalkapalloa seuranneilta, kun kovaäänisesti piipittävä hätätiedote osui pelilähetyksen päälle. [HS, 2010]. Tilannetta ei parantanut uuden vaaratiedotelain voimaantulo kesällä 2013, vaan valtakunnallisten vaaratiedotteiden määrä on kasvanut entisestään.

Viranomaisten heikkoa Internet-läsnäoloa kriisitilanteissa on niin ikään ihmetelty Aasian tsunamista lähtien. Vaikka nykyään verkkoon tiedotteita saadaankin, niin viranomaisten verkkopalvelut voivat edelleen kaatua saman tien suuren kuormituksen alla, kuten kävi poliisin ja Sisäasiainministeriön verkkopalvelulle vielä marraskuussa 2011 poliisin julkaistessa listan vuodetuiksi epäillyistä verkkopalvelutunnuksista. Vaikka sivujen tekniikkaa päivitettiin 2004

tsunamin jälkeen, ei se siltikään kestänyt kymmenien tuhansien yhtäaikaisten kävijöiden aiheuttamaa kuormituspiikkiä. Huolestuttavana pidän, että poliisin tietohallintopäällikön mukaan sivuille ei edelleenkään luvata kuormankestävyyttä vastaavissa tilanteissa uudistuksista huolimatta [Vanhala, 2011]. Valtioneuvoston kanslia puolestaan hankki vuonna 2005 verkko-osoitteen *Tilannekuva.fi*, jonne oli tarkoitus pystyttää viranomaisten yhteyden kansalaisia etenkin kriisitilanteissa palveleva verkkoportaali. Osoitteeseen ei kuitenkaan ole rakennettu mitään sisältöä, eikä tällaisesta ole nykyisellään suunnitelmia. Tietoverkkojen kansalaisvaikuttamisesta, ”verkkovoimasta”, väitöskirjaansa valmisteleva Kari A. Hintikka ehdottaakin palkitussa Apps4Finland 2011 -kilpailutyössään [Hintikka, 2011], että palvelusta kehitettäisiin viranomaisten, joukkoviestinten ja kansalaisten yhteinen sisältöalusta, johon keskitetysti aggregoitaisiin avointa viranomaisten tuottamaa dataa, median uutisia sekä kansalaisten omia havaintoja.

Viranomaistiedottamisessa on havaittu monia muitakin ongelmia, kuten kuka tiedotteita saa antaa, ja millä kielillä tiedotteet tulee julkaista. LVM:n ohella asiaa on selvitellyt aktiivisimmin viime aikoina Sisäasiainministeriön pelastusosasto. Vuoden 2010 alkupuolella toiminut VIRANTA-työryhmä päätyi loppuraportissaan [SM, 2010a] esittämään kuutta toimenpidettä, mukana hätätiedotteiden antaminen alueellisesti, kohdennetun viranomaistiedotteen kehittäminen sekä uuden viestintäteknologian suunnitelmallisempi hyödyntäminen. Raportin lausuntopyyntökierroksella alueellisia tiedotteita kommentoi ainoastaan Tampereen aluepelastuslaitos, joka puolusti tiedotteiden lähettämistä valtakunnallisesti tiedotteiden vähäisellä kokonaismäärällä, tunnettavuuden lisäämisellä ja matkustavien tavoittamisella [SM, 2010b]. Kohdennettujen viranomaistiedotteiden kohdalla puolestaan toistuu tuttu lausahdus järjestelmän toteuttamisen kannattamisesta ja samaan hengenvetoon rahoituksen puutteesta, tällä kertaa Hätäkeskuslaitokselta. Eniten innostusta on herättänyt uusien viestintäkanavien käyttö, jota eri pelastuslaitokset jo nyt toteuttavatkin, joskin hyvin erilaisin tavoin. Pohjois-Karjalan pelastuslaitos visioikin kommenteissaan Hintikan Tilannekuva.fi:n kaltaista verkon yhteisöpalvelua.

Kenties pitkälti näiden lausuntojen myötä SM:n keväällä 2011 asettama viranomaistiedotteiden antamisesta lakialoitetta valmisteleva työryhmä ei lopulta sisällyttänyt lakiehdotukseensa mitään muuta uusista viestintätavoista kuin viittauksen olemassa olevaan Sähköisen viestinnän tietosuojalakiin (516/2004), johon lisättiin 2006 velvoite teleyrityksille välittää kohdennettuja viranomaistiedotteita. Uusi laki vaaratiedotteesta (466/2012) tuli voimaan kesäkuussa 2013, mutta sen suurin muutos oli vain vaatimus tiedotteiden kääntämisestä ruotsiksi – mitä viranomaiset ovat jo ehättäneet arvostelemaan tiedotteiden välittämistä

hidastavana [TS, 2012]. Vaikka on toki tärkeää, että kansalaiset saavat viranomaispalvelunsa ja etenkin hengenvaarasta varoittavat tiedotteet omalla äidinkielellään, ihmettelen silti, onko hätätiedoteasiassa harhauduttu sivupolulle siitä, miten yleensä kansalaiset parhaiten saataisiin tavoitettua hätätilanteessa – kielestä, viestintäkanavasta tai sijainnista riippumatta.

1.2. Vaaratiedottaminen – tekninen vai yhteiskunnallinen haaste?

Tämä tutkielma selvittää uusien tieto- ja viestintäteknologioiden mahdollisuuksia viranomaisten vaaratiedottamisen parantamisessa. Tietojenkäsittelytieteen tutkielmana tarkastelunäkökulma on ensisijaisesti vaaratiedotteiden välittämiseen tarkoitetun järjestelmän tutkimisessa. Selvitän, millaisia vaatimuksia tällaiselta järjestelmältä edellytetään, esitän erään arkkitehtuuriluonnoksen toteutusvaihtoehdoksi ja arvioin tätä käyttövaatimuksia vasten.

Viranomaisilla tarkoitan vaaratiedotelain (466/2012) viidennessä pykälässä listattuja toimijoita, joilla on toimivalta vaaratiedotteen antamiseen. Toisaalta etenkin merkittävissä tilanteissa korostuu yhteistoiminta muidenkin yhteiskunnan toimijoiden kanssa. Lisäksi viestintäteknologian lainsäädännön kehittämisen osalta Liikenne- ja viestintäministeriöllä (LVM) on merkittävä rooli. Vastaavasti näiden viranomaisten viestinnässä tarkastelun painopiste on tilanteissa, joissa vaaratiedotelain kolmannen pykälän mukaan tiedotetaan *"silloin kun vaarallisen tapahtuman seurauksena voi aiheutua ihmisille hengen- tai terveysvaaraa taikka vaara merkittävälle omaisuuden vaurioitumiselle tai tuhoutumiselle"*. Ennen vuoden 2012 vaaratiedotelakia käytettiin termejä *hätätiedote* ja sitä lievempi *muu viranomaistiedote*, joilla oli mm. erilaiset vaatimukset viestin välittämiselle.

Tietoyhteiskunnassa myös viranomaisviestinnän olisi luontevaa hyödyntää modernin tieto- ja viestintäteknologian mahdollisuuksia. Perinteisesti hätätiedotteita on välitetty joukkoviestimien eli radion ja television välityksellä. Näiden rinnalle ovat 1990- ja 2000-luvun aikana nousseet matkaviestimet sekä Internet. Nämä puolestaan ovat edelleen yhdistymässä siten, että yhä useampi matkaviestinlaite on ns. älypuhelin, joka mahdollistaa myös Internetin käytön missä tahansa verkon kuuluvuusalueelta. Matkaviestimillä Internetiä käyttääkin jo yli neljännes kansalaisista [Tilastokeskus, 2011]. Matkaviestimet eivät ole pelkästään passiivisia vastaanottimia radioiden ja televisiolaitteiden tapaan, vaan ne kommunikoivat aktiivisesti verkon kanssa silloinkin, kun laitteen käyttäjä ei tee laitteella mitään toimintoa. Toisaalta laitteet voivat itsekin selvittää eri tavoin tarkasti oman sijaintinsa. Näiden ominaisuuksien myötä matkaviestimiä voitaisiin käyttää paitsi tavoittamaan henkilökohtaisesti kansalaiset, myös rajaamaan viestin kohdejoukko maantieteellisesti tietylle alueelle. Kuten edellisestä kohdasta käy ilmi, näitä mahdollisuuksia ei ole vielä juurikaan käytän-

nössä hyödynnetty. Tutkielmassa pyrinkin selvittämään, missä määrin teknologian rajoitukset ovat olleet ongelmana, ja toisaalta etsimään uusia mahdollisuuksia viranomaisviestintään.

Tarkastelen myös vaaratilanteisiin liittyvän viestinnän luonteen muuttumista yhteiskunnassa tieto- ja viestintäteknologian kehittymisen myötä. Kun aiemmin viesti levisi viranomaislähteestä median ja joukkoviestimien kautta yksisuuntaisesti yleisölle, nykyään tämän rinnalle on syntynyt kansalaisten keskinäisen sähköisen viestinnän myötä *sosiaalinen media*, jossa kuka tahansa voi toimia tiedontuottajana mielivaltaisen laajalle yleisöjoukolle. Tällaisessa mediassa viestit leviävät niiden kiinnostavuuden perusteella, eivätkä levittäjät aina arvioi viestin paikkansapitävyyttä. Tällainen ”sähköinen puskaradio” haastaa viranomaisten oman viestinnän, sillä epämääräiset huhut ja virheellinenkin tieto leviävät salamannopeasti. Toisaalta jos viranomaiset olisivat itse läsnä sosiaalisen median palveluissa ja tiedotteet välitettäisiin suoraan myös niiden kautta, saataisiin palveluihin luontevasti niiden omilla välineillä levitettäväksi oikeaakin tietoa ilman välikäsiä. Esimerkiksi Kuntaliiton julkaisemassa verkkoviestintäohjeessa [Kuntaliitto, 2010] korostetaan sosiaalisen median hyötyjä normaalissa kunnalliseen päätöksentekoon osallistumisessa, mutta toisaalta sen käytöstä kriisiviestinnässä ei vielä ole käytännön esimerkkejä.

Seuraavassa luvussa esittelen tutkielman lähteinä käytettyä materiaalia, viranomaisviestinnän määrittelyä viranomaisten itsensä toimesta sekä aiempaa tutkimusta viranomaisviestinnän kehittämisestä sekä viestintäteknologioiden hyödyntämisestä hätäviestitarkoituksiin. Luvussa 3 sukelletaan GSM- ja UMTS-matkaviestinverkkojen tekniseen toteutukseen erityisesti paikantamisen ja sijantipohjaisten palveluiden kannalta. Tämän ohessa käyn myös lyhyesti läpi viranomaisten Internet-palveluiden teknistä taustaa. Tämän jälkeen luvussa 4 kuvaan vaaratiedotteiden välitysjärjestelmää ulkomaisten hankkeiden pohjalta. Viidennessä luvussa esitän näistä johdetut vaatimukset ja erään esimerkkiarkkitehtuurin Suomeen soveltuvalle tietojärjestelmälle viranomaistiedotteiden julkaisuun ja välittämiseen eri kanavien kautta. Kuudennessa luvussa kuvataan tietojärjestelmän arkkitehtuurin analysointia ATAM-menetelmällä sen laadun arvioimiseksi. Lopuksi luvussa 7 kokoan yhteen havaintoja ja esitän joitakin ajatuksia aihealueen tulevaisuuden kannalta.

2. Aineisto ja tutkimuksen toteutus

2.1. Aineistosta, rajauksesta ja valintaperusteista

Tutkielman lähdeaineisto jakautuu yleisesti viranomaisten vaara- ja kriisitiedottamista ja sen kehitystä koskeviin lähteisiin, verkkoteknologiaa ja erityisesti paikantamista koskeviin lähteisiin sekä muuhun lähdekirjallisuuteen.

Viranomaisten ja kansalaisten välisen viestinnän teknistä kehitystä ja murrosta informaatioyhteiskunnassa on tutkittu jonkin verran. Kotimaisessa kentässä motivaationa ovat olleet usein viranomaistiedotuksen kompastukset erilaisten onnettomuuksien yhteydessä, esimerkiksi Aasian tsunamikatastrofin jälkeen tai Nokian vesikriisin kohdalla [Seeck *et al.*, 2008]. Lähimpänä aihetta kotimaisista tutkimuksista on ollut Jyväskylän yliopistossa 2012–2013 toteutettu nk. Sapporo-hanke (*Situational Awareness Through Proactive Risks and Opportunities*), jossa tutkittiin ja kehitettiin yhteistyössä viranomaisten kanssa prototyyppi älypuhelinsovelluksesta hätäviestinnän parantamiseen [Kuula *et al.*, 2013]. Kaikkein tuoreinta kotimaista tutkimustietoa edustaa Pelastusopiston ja Poliisiammattikorkeakoulun vuonna 2013 toteuttama ja päällekkäin oman työni kanssa edennyt tutkimus *"Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa"* [SM, 2014]. Valitettavasti hanke tuli tietooni vasta, kun valtaosa omasta työstäni oli jo valmiina, mutta sen loppuraportti sekä väliraporttijulkaisut [Hokkanen *et al.*, 2013] ja [Pylväs *et al.*, 2014] vahvistavat useimmat omat päätelmäni ja täydentävät niitä. Hankkeen julkaisuissa määritellään myös omaa työtäni kattavammin hätätilanteen elinkaari sekä viranomaistoiminnan ja -viestinnnän lähtökohdat.

Pääasiallisesti aiheesta löytyvä aiempi materiaali on kuitenkin viranomaisten itse tuottamia selvityksiä, jotka ovat usein tarkastelunäkökulmaltaan varsin rajallisia ja ehdotuksissaan varovaisen konservatiivisia. Laajimmin sijaintiin perustuvaa, monikanavaisen hätäviestinnän kehittämistä ovat tutkineet australialaisessa Wollogongin yliopistossa Anas Aloudat ja Katina Michael. He ovat mm. selvittäneet [Aloudat *et al.* 2007], millaisia erilaisia sijaintiin pohjautuvia hätätilanteiden hallintahankkeita on eri puolilla maailmaa. Vastaavasti Kidd ja muut [2008] ovat kartoittaneet Uuden-Seelannin tarpeisiin matkaviestinverkkoihin pohjautuvia varoitusteknologioita. Nämä selvitykset antavat hyvän vertailupohjan Suomessa käydylle keskustelulle kohdennetuista viranomaistiedotteista (VIRVA-työryhmä). Aloudat ja Michael [2011] ovat myös tutkineet sijaintipohjaisia monikanavaisia hätätiedotusjärjestelmiä ja muotoilleet pohjaa tällaisen käyttöönotolle Australiassa.

Matkaviestimiin lähetettävistä hätäviesteistä on kotimaisen VIRVA-työryhmän lisäksi käynnissä laajempia kansainvälisiä hankkeita, joiden lähtökohdat tosin poikkeavat hieman toisistaan. Näillä on oletettavasti merkittävä vaikutus siihen, millaisia uusia toiminnallisuuksia valmistajat lähitulevaisuudessa toteuttavat päätelaitteisiin ja verkkoon. Yksi merkittävimmistä on yhteiseurooppalainen EU-ALERT, jonka taustalla on Euroopan telekommunikaatioalan standardijärjestö ETSI. Siinä kohdennettujen viestien lähetys perustuu CBS-tekniikkaan sekä joukkoviestimissä välitettäviin tiedotteisiin. EU-ALERT on sisällytetty mukaan 3GPP Release 11:een. Toinen vastaava hanke on japanilaisten Earthquake and Tsunami Warning Service (ETWS), jonka erikoisuutena on automaattinen ensitiedotteen lähettäminen heti, kun järistys havaitaan. EEWS oli mukana jo 3GPP Release 8:ssa ja on sittemmin yhdistetty yleiseen 3GPP:n PWS (Public Warning System) -määritykseen Release 11:ssä. Kolmas, kenties nopeimmin etenevä ja eniten laitevalmistajilta tukea saava hanke on yhdysvaltalaisten CMAS/WEA (Commercial Mobile Alert System, nykyään myös Wireless Emergency Alerts). Se eroaa toteutukseltaan kahdesta edellisestä sikäli, että vaatimuksissa päätelaitteiden tulee tukea erikseen CMAS/WEA-viestien vastaanottoa ja esittää viestin saapuessa normaalista tekstiviestistä poikkeava hälytysääni, joka riippuu viestin kolmiportaisesta vakavuustasosta [Hietalahti *et al.*, 2010]. Muita lähdekirjallisuudessa mainittuja hankkeita on käynnissä mm. Israelissa ja Chilessä.

Matkaviestinverkkojen teknologian osalta peruslähteinä ovat olleet monien muiden opinnäytetöiden tapaan Jyrki Penttisen tietoliikennetekniikan perusteita käsittelevät kirjat [Penttinen, 2006a; 2006b]. Nämä esitykset ovat kuitenkin melko pinnallisia, ja löytyipä teoksista selkeitä asiavirheitäkin. Näiden lisäksi verkon referenssiarkkitehtuurista on toki saatavilla 3GPP:n tekniset määritykset, jotka useimmiten olivat liiankin yksityiskohtaisia tämän työn tarpeisiin. Määritykset eivät myöskään takaa, että kaikki niissä esitetyt toiminnallisuudet on toteutettu samalla tavalla eri valmistajien verkkolaitteissa tai operaattoreiden verkoissa.

Paikantamisesta matkaviestinverkossa on olemassa paljoltikin opinnäytetyötasoisia tutkielmia viimeisen kymmenen vuoden ajalta. Vaikka monet näistä keskittyvät yleensä muihin sijaintipohjaisiin palveluihin kuin verkkopohjaiseen paikannukseen, on tämäkin vaihtoehto tavallisesti esitelty lyhyesti – usein mainiten sovelluksena viranomaisten kohdennetut hätätiedotteet. Näissä töissä ei kuitenkaan yleensä ole menty kovin syvälle verkkopohjaisen paikantamisen tekniseen toteutukseen, eikä etenkään viranomaistiedotepalvelun vaatimaan suurten käyttäjämäärien nopeaan paikantamiseen. Parhaiten alueellisten käyttäjien selvittämistä on kuvattu Paukkosen [2005] insinöörityössä, jossa tehtä-

vänanto liittyi matkailupalvelujen kehittämisprojektiin ja verkosta haluttiin louhia tietoa päätelaitteiden liikkeistä vertailtavaksi muita tilastotietoja vasten. Työssä esitetyt menetelmät muodostavat kuitenkin perustan myös passiiviselle sijaintitiedon seurannalle, jota tarvitaan, jos halutaan tietää kaikki tietyllä alueella olevien päätelaitteiden liittymänumerot.

Muista merkittävistä projekteista enemmän kuriositeetiksi jäänee Internetin teknisiä suosituksia kehittävän IETF:n (*Internet Engineering Task Force*) alaisuudessa parin vuoden ajan toiminut ATOCA-työryhmä (*Authority-to-Citizen Alert*), joka pyrki määrittämään hätätiedotteiden välitysjärjestelmää yleisesti Internetiin liitettäville laitteille [IETF, 2012]. Sen toiminta jäi kuitenkin melko pienimuotoiseksi, enkä pidä odotettavana, että ATOCA-ryhmän esittämän luonnoksen toteuttavia laitteita tai ohjelmistoja tulisi lähiaikoina laajamittaisesti markkinoille. Sosiaalisen median, kuten Twitterin ja Facebookin, käyttämistä hätäviestien lähettämiseen ovat puolestaan selvittäneet ainakin yhdysvaltalaiset Woodcock [2009] ja Barnett [2011]. Twitterin kautta levitetyn tiedon hyödyntämistä onnettomuuksissa tilanteiden hahmottamiseksi ovat analysoineet Vieveg ja kumppanit [2010] sekä empiirisesti Bostonin maratonin pommiiskujen jälkeen Starbird ja kumppanit [2013]. Tämä alue on kuitenkin toistaiseksi vielä huomattavasti vähemmän tutkittua sijaintipohjaisiin järjestelmiin verrattuna, joskin toisaalta yleisemmällä tasolla tutkimusta sosiaalisen median erilaisista mahdollisuuksista on tehty runsaasti. Näihin en kuitenkaan tämän tutkielman puitteissa perehdy enempää.

2.2. Tutkimusongelma ja keskeiset käsitteet

Tarkoitukseni oli alun perin tutkia tekstiviestipohjaisen hätätiedottamisen ongelmia puhtaasti teknologian näkökulmasta matkaviestinverkkojen teknisen dokumentaation ja aiemman tutkimuksen pohjalta. Alkuperäinen oletukseni oli, että järjestelmän käyttöönottoon liittyvät ongelmat ovat olleet juuri teknologiasta joko suoraan (nykyiset verkot eivät joko tarjoa lainkaan mahdollisuuksia massapaikantamiseen tai ovat liian hitaita siihen) tai välillisesti (toteutus vaatisi mittavia lisäinvestointeja uuteen laitteistoon) johtuvia. Tällöin ratkaisuna voisi olla kokonaan uudet teknologiset ratkaisut tai vaihtoehtoiset lähestymistavat vaaratiedotteiden toteutukseen.

Työn edetessä alkoi kuitenkin vaikuttaa siltä, että ongelma ei ole pelkästään teknologiaan liittyvä, vaan taustalla vaikuttaa myös laajempi ilmiö viranomaisviestinnän muutoksesta. Heräsi kysymys, onko kaikkien vaara-alueella olevien kansalaisten tavoittamiseen pyrkivä massatekstiviestijärjestelmä edes enää järkevä vaihtoehto, vai pitäisikö keskittyä jo seuraavien teknologioiden

tuomiin mahdollisuuksiin. Toisaalta huomionarvoista on koko vaaratiedottamisen prosessi, ei pelkästään varoitusviestin toimittaminen kansalaisille. Kansainvälinen kehitys vaihtoehtoisten ja kattavampien teknologioiden myötä vaikuttaa myös väistämättä siihen, millaisia ratkaisuja Suomessa lopulta otetaan käyttöön. Näin ollen tutkimuskysymyksiksi kiteytyivät lopulta seuraavat:

1. Mitkä ovat monikanavaisen vaaratiedotejärjestelmän tekniset vaatimukset?
2. Millainen on tällaisen järjestelmän arkkitehtuuri?
3. Miten järjestelmä soveltuisi käyttöön Suomessa?

Tutkielman aihealueeseen liittyy joukko olennaisia käsitteitä, joiden avaaminen valottaa myös tutkimusongelmaa. Keskeisin on termi *vaaratiedote*, jonka määrittelemiseksi siteeraan suoraan lakia vaaratiedotteista (2 §):

> ”Vaaratiedote on toimivaltaisen viranomaisen antama tiedote, jonka tarkoitus on varoittaa vaarallisesta tapahtumasta ja jolla annetaan toimintaohjeita.”

Lain kolmas pykälä puolestaan määrittää, millaisissa tilanteissa vaaratiedotteita käytetään:

> ”Vaaratiedote voidaan antaa, jos se on välttämätöntä väestön varoittamiseksi, silloin kun vaarallisen tapahtuman seurauksena voi aiheutua ihmisille hengen- tai terveysvaara taikka vaara merkittävälle omaisuuden vaurioitumiselle tai tuhoutumiselle.
>
> Vaaratiedote voidaan lisäksi antaa, kun vaaratilanne, jonka perusteella vaaratiedote on annettu, on ohi.”

Näiden ohella käytän vaaratiedotteen synonyymina termiä *hätätiedote*, jolla vaaratiedotteita myös Suomessa ennen vuoden 2012 vaaratiedotelakia kutsuttiin. Periaatteessa uusi laki teki hätätiedotteesta vaaratiedotteen alakäsitteen yhdistäessään sen ja aste-eroltaan lievemmän *muun viranomaistiedotteen* yhteisen termin ja lakitekstin alle. Toisaalta aiempi erottelu oli vain Suomea koskeva erikoistapaus ja ulkomailta löytyy vastaavasti omia vaaratiedotelaista poikkeavia käyttötapoja ja jaotteluja. Yleisesti *yleisövaroitusjärjestelmiä* (public alert system tai public warning system) voidaan esimerkiksi Yhdysvalloissa käyttää siepatuista lapsista tiedottamiseen (AMBER alert) ja monissa Aasian maissa ensisijainen käyttötarkoitus on hyökyaalloista ja maanjäristyksistä varoittaminen. Huomionarvoista on myös, että vaaratiedotelain määritelmä ei sisällä monessa muussa yhteydessä käytettyä määritystä siitä, että vaara uhkaisi välittömästi. Tämä on tärkeää siksi, että välittömyyden ehto rajaisi pois hitaammin kehittyvät mutta mahdollisesti yhtä vaaralliset tilanteet (esim. poikkeuksellisen voimakkaat sääilmiöt).

Alkuperäistä tutkimusongelmaa, eli kohdennettujen vaaratiedotteiden teknisiä mahdollisuuksia, tarkastelen ennen kaikkea mobiiliverkoissa tarjottavien *sijaintipohjaisten palveluiden* (location-based service, LBS) kautta. Suomen-

kielisessä kirjallisuudessa käytetään myös vaihtoehtoisia suomennoksia *paikkasidonnaiset palvelut* tai *paikkaperustaiset palvelut*. Nämä kaikki tarkoittavat käyttäjän sijaintietoa hyödyntäviä palveluita, joista kohdennetut viranomaistiedotteet ovat yksi sovellus monien kaupallisten palveluiden ohella. Paikkatieto itsessään voidaan selvittää monin eri tavoin, joita kuvataan tarkemmin kohdassa 3.2.

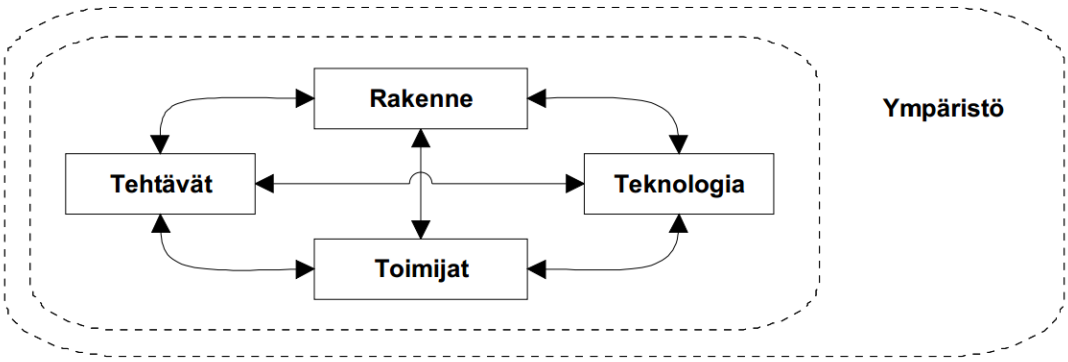
Verkkopalvelut puolestaan ovat Internetin välityksellä käytettäviä tietopalveluita, käytännössä yleensä World Wide Web -palveluun toteutettuja *verkkosivustoja*, joihin päästään HTTP-protokollaa tukevalla selainohjelmistolla. Nykyään verkkopalvelut voivat tarjota entistä enemmän myös interaktiivista sisältöä ja palveluiden ylläpitäjät voivat viestiä niiden kävijöiden kanssa.

Sosiaalinen media on yleiskäsite Internetin välityksellä käytettäville verkkopalveluille, joissa pääpaino on käyttäjien tuottamalla sisällöllä ja viestinnällä. Ne eroavat perinteisistä verkkopalveluista siinä mielessä, että ne toimivat ennen kaikkea palvelun käyttäjien tuottaman materiaalin levitysalustana eivätkä itse juurikaan tuota sisältöä. Tällä hetkellä suosituimpia sosiaalisen median palveluita ovat yhteisösivusto Facebook ja lyhytviestipalvelu Twitter, joita molempia voi myös käyttää luontevasti älypuhelimilla.

Lopuksi *vaaratiedotteiden välitysjärjestelmällä* tarkoitan tietojärjestelmää, jonka tarkoituksena on välittää vaaratiedotteet niiden lähettäjän määrittelemälle kohdejoukolle tai alueelle erilaisten välityskanavien avulla. Tietojärjestelmän toteutuksesta ja siihen liitetyistä muista järjestelmistä riippuen kanavia voivat olla esimerkiksi televisio, radio, verkkopalvelut, mobiilihälytykset ja sosiaalinen media.

2.3. Tutkimusmetodista ja luotettavuudesta

Tietojärjestelmätieteen tutkimuksessa on mukana teknologian lisäksi myös inhimillinen ulottovuus tietojärjestelmiä käyttävien ihmisten ja organisaatioiden toiminnassa. Tutkimusmetodiksi ei siksi yleensä sovi yhtä suoraviivainen empiiriseen tutkimukseen perustuva metodi kuin esimerkiksi algoritmiikassa tai ohjelmistotuotannossa, jossa tulokset ovat selkeämmin mitattavissa. Tietojärjestelmätieteen tutkimus nojautuu myös vahvasti liiketoiminnallisiin näkökulmiin, jolloin tutkimusmetodit ovat usein samoja kuin talous- ja johtamistieteissä. Tietojärjestelmien tutkimus onkin usein hyvin poikkitieteellistä ja sijoittuu näiden kolmen osa-alueen leikkauskohtaan. Alan tutkimusmenetelmät voidaan karkeasti jakaa suunnittelutieteelliseen, luonnontieteelliseen ja käyttäytymistieteelliseen lähestymistapaan.



Kuva 1. Organisaation peruselementit ja niiden välinen vuorovaikutus Leavittin timanttia mukaillen Scottin 1987 esittämänä varianttina [Nurminen et al., 2002]

Tietojärjestelmät eivät ole muusta organisaatiosta irrallisia, vaan vaikuttavat kiinteästi sen muuhun toimintaan. Organisaation toimintaa voidaan tarkastella sosio-teknologisella näkökulmalla ns. Leavittin timantiksi kutsutun mallin mukaan, joka selittää toimintaa neljän erillisen tekijän (tehtävät, teknologia, toimijat ja rakenne) kokonaisuutena (ks. kuva 1). Muutokset jollakin osa-alueella vaikuttavat lähes aina myös kaikkiin muihin, joten mallia onkin usein käytetty juuri muutosvastarintaa kuvattaessa. Nurmisen ja muiden [2002] mukaan uuden tietojärjestelmän käyttöönotto vaikuttaa lähes aina myös tehtävien suoritustapaan, muuttaa toimijoiden osaamisvaatimuksia sekä saattaa vaikuttaa työnjakoon ja yhteydenpitoon ympäristön kanssa.

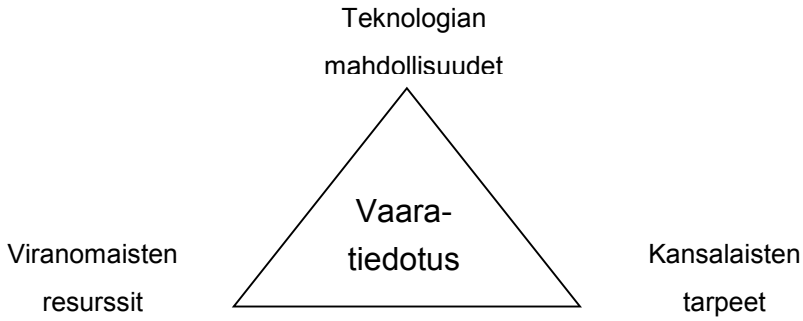
Tässä tutkielmassa käyttämäni metodi nojaa suunnittelutieteen menetelmiin. Konstruktiivinen tutkimus on soveltavaa tutkimusta, jossa konstruktiolla tarkoitetaan konkreettisen käytännön ongelman ratkaisua tieteellisissä puitteissa. Järvisen ja Järvisen [2011] mukaan suunnittelutietämys koskee *kohteen*, *toteutuksen* ja *prosessin* (eli *metodin*) suunnittelua. Kohteen suunnittelu on lopputuloksen suunnittelua ja määrittelyä (spesifiointia), prosessin suunnittelu on sen suunnittelua, miten periaatteessa eri resursseja käyttäen lopputulos saataisiin aikaan, ja toteutuksen suunnittelu on käytännön suunnittelua, miten alkutilasta päästään haluttuun lopputilaan. Keskityn itse tässä työssä pääsääntöisesti kohteen (eli vaaratiedotteiden välitysjärjestelmän) spesifiointiin, sillä konkreettisen toteutuksen ja prosessin suunnittelu on tällaisen tutkielman laajuuden ulkopuolella.

Eräänä esimerkkinä suunnitteluttutkimuksen metodeista Järvinen ja Järvinen kuvaavat Peffersin ja muiden [2007] laatiman suunnitteluttutkimuksen metodologian, jossa tieteellinen suunnitteluttutkimuksen raportointi jaetaan seuraaviin kuuteen aktiviteettiin: 1) ongelman tunnistaminen ja lukijan motivointi, 2) ratkaisun tavoitteiden määrittely, 3) suunnittelu ja toteutus, 4) demonstrointi, 5) arviointi ja 6) julkistaminen. Olen rakentanut oman työni osittain tätä mallia

noudattaen: ongelman on helposti tunnistettavissa ja motivaatio tutkimukselle ja ratkaisun löytämiselle löytyy asian yleishyödyllisyydestä. Ratkaisun tavoitteet puolestaan muodostavat keskeiset tutkimuskysymykset ja ne ovat suoraan johdettavissa tutkimuksen ongelmanasettelusta. Edelleen esitän suunnitelman ja erään toteutuksen ratkaisulle aiempaan tutkimukseen pohjautuen. Tämän työn laajuudessa en kuitenkaan toteuta juurikaan demonstrointia tai arviointia, vaan nämä osa-alueet kattaa yhteenvetoluku.

Aineistoon tutustuessani havaitsin selkeästi, että aihealueen tarkastelutavat ovat hyvin kahtiajakautuneet. Verkon paikannusteknologian ja ryhmäviestien ominaisuuksia analysoivat tutkimukset olivat usein optimistisia tekniikan suomista mahdollisuuksista ja visioivat rohkean avoimesti uusia käyttösovelluksia, kuten esimerkiksi alueellisen kävijämäärän seuraaminen matkailualueella [Räsänen *et al*., 2005]. Vaikka tämän kaltaisia yksittäisiä kokeiluprojekteja onkin tehty maailmalla useita, verkkopohjaisten paikkatietojen hyödyntäminen on jäänyt vähäiseksi. Tämän ilmiön syihin palaan myöhemmin.

Viranomaisten toimintaa ja viestintää käsittelevät tutkimukset ovat yleensä sen sijaan melko sulkeutuneita ja nojaavat vahvasti viranomaisten velvollisuuksiin, resursseihin ja muihin rajoitteisiin. Viranomainen ei innovoi uutta, vaan pyrkii hoitamaan olemassa olevat lakisääteiset velvollisuutensa toimiviksi havaituin vakiintunein käytännöin. Viestintä koetaan toissijaiseksi tukitoiminnoksi viranomaisten varsinaisten tehtävien (esim. pelastustoiminta) rinnalla. Vaikka sen merkitys päätehtävän kannalta olennaisen kansalaisten ohjeistamisen ja tiedottamisen kannalta onkin selvä, viestinnän nähdään silti palvelevan lähinnä median ja sitä kautta kansalaisten yleistä uteliaisuutta uutiskynnyksen ylittävistä tapahtumista [Rantala, 2007]. Viestintäteknologian nopea kehittyminen ja arkipäiväistyminen ovat luoneet *sosiaalisen median* käsitteen perinteisen median rinnalle ja muuttaneet tiedonvälityskanavien ja tiedon leviämisen luonnetta [Hintikka, 2010]. Nämä uudet viestintäkanavat hyppäävät täyttämään kansalaisten tiedontarpeita etenkin silloin, kun tietoa ei ole saatavilla perinteisistä, virallisemmista kanavista. Tähän kehitykseen on herätty jo yrityksissä, mutta viranomaispuolella muutos on hitaampaa ja varovaisempaa.



Kuva 2. Tutkielman tarkasteluympäristö

Tutkimuksen yhdeksi keskeiseksi motivaattoriksi nousikin teknologian roolin pohdinta viranomaisten ja kansalaisten välisessä tiedonvälityksessä – sekä viranomaisten tiedottamisessa että kansalaisten keskinäisessä ja viranomaisia täydentävässä viestinnässä (Kuva 2). Teknologia on toisaalta sekä mahdollistaja uusien, tehokkaampien viestintätapojen tai viestien kohdennuksen osalta, mutta toisaalta myös rajoittaja, jos viestinnän osapuolten odotukset sen hyödyntämisestä eivät kohtaa. Vaaratiedotteet on mielikuvissa ja esimerkeissä yleensä liitetty vain merkittäviin suuronnettomuuksiin tai luonnonkatastrofeihin, kuten maanjäristyksiin tai ydinvoimalaitoksen onnettomuuteen. Kuitenkin tiedotteita on viime aikoina käytännössä annettu teknologian rajoituksista johtuen valtakunnan tasolla melko vähäpätöisistä ja alueellisista uhista. Viestintäteknologian kehittyessä ja vastaanottajajoukon tarkentuessa tiedotteiden lähetyskynnys voi edelleen laskea. Valtakunnallisissa televisiolähetyksissä leviävät varoitukset yksittäisestä karhusta voivat tuntua jo liiankin matalalta varoituskynnykseltä, mutta ideaalitilanteessa viesti pystyttäisiin välittämään vain sille alueelle, jossa todellinen uhka on olemassa.

2.4. Työn kulku

Aluksi kävin läpi mobiiliverkkojen teknistä toteutusta, etenkin sijaintipohjaisia palveluita, ja tähän liittyviä vaaratiedotesovelluksia. Samoin tarkastelin yleisellä tasolla korkean käytettävyyden verkkopalvelujen toteutuksia sekä Suomen viranomaisten nykyisiä verkkopalveluita. Lähdin määrittelemään varsinaista vaaratiedotejärjestelmää ulkomaisten vastaavien hankkeiden kautta, joista keskeisimmät löytyivät niin 3GPP:n standardeista kuin aihealueen tutkimuksestakin. Näiden pohjalta hahmottuivat Suomen oloihin sopivan vaaratiedotejärjestelmän vaatimukset sekä toimintaympäristö.

Vaatimuksiin pohjautuen määrittelin korkean tason arkkitehtuuritoteutuksen esimerkkijärjestelmästä, joka toteuttaisi vaaditut avaintoiminnot viestinvälityksessä. Järjestelmän teknisessä kuvauksessa ei ole menty syvälle itse järjestelmän sisäisiin toimintoihin, koska ne riippuvat lopullisesta toteutukseen valitusta tekniikasta. Matkaviestinverkkojen sekä web-julkaisuteknologian osalta pohjaudutaan siihen tekniseen kuvaukseen, joka työssä on aiemmin esitetty.

Esitettyä järjestelmäarkkitehtuuria tarkastelin yleisellä tasolla ATAM-menetelmän avulla, joka pyrkii arvioimaan ohjelmistoarkkitehtuuria sen laatuvaatimuksia vasten. ATAM-arviointi formaalina prosessina toteutetaan yleensä ryhmätyönä, johon osallistuu laajalti sekä asiakkaan, loppukäyttäjän, ohjelmiston suunnittelijoiden että toteuttajien edustajia. Tämän tutkielman puitteissa ei kuitenkaan ollut mahdollista eikä mielekästä toteuttaa tällaista kokoontumista, joten olen pyrkinyt käyttämään ATAM-menetelmästä soveltuvia osia itse, tutkien mahdollisimman objektiivisesti eri näkökulmista esitettyä arkkitehtuuria.

3. Viestintäjärjestelmien tekninen tausta

"Viestintä yleensä epäonnistuu - paitsi sattumalta."
Wiion 1. laki inhimillisestä viestinnästä [Wiio, 2013]

Mobiiliverkoilla ei ole jatkuvaa tarkkaa tietoa päätelaitteiden sijainneista. Soluverkko tietää päätelaitteen sijainnin summittaisesti isomman alueen tarkkuudella ja ainoastaan silloin, kun päätelaite on aktiivinen (lähettää tai vastaanottaa viestiä kuten puhelua), verkko selvittää tarkemman solukohtaisen sijainnin. Tämäkään ei vielä välttämättä riitä paikantamisen perusteeksi, sillä haja-asutusalueella solutarkkuus voi olla useita kilometrejä. Päätelaite ei myöskään aina kommunikoi sitä lähimpänä olevan tukiaseman kanssa. Julkisuudessa verkkopaikantamisen tarkkuusongelmat olivat mm. Tampereella kesällä 2011 kadonneen tytön etsintöjen yhteydessä, kun tytön puhelin paikantui yli kymmenen kilometrin päässä olleeseen tukiasemaan [Aamulehti, 2011].

Matkaviestimien ohella Internet ja WWW ovat myös arkipäiväistyneet yhä laajemman kansalaisjoukon käyttämiksi. Suosituimmat sivustot ovat interaktiivisia miljoonia yhtäaikaisia käyttäjiä palvelevia sovelluksia. Erilliset asiakasohjelmistot vähenevät ja sovellukset siirtyvät yhä enemmän käytettäväksi yhtenäisen selainohjelmiston välityksellä. Sähköpostin aloittamaa tietä seuraavat tekstinkäsittely- ja taulukkolaskentaohjelmat. Tätä kehitystä vasten monet viranomaisten kansalaisille tarkoitetut verkkopalvelut seuraavat valitettavan hitaasti perässä. Vanhanaikaisten julkaisujärjestelmien päälle rakennetut sivustot eivät kestä kuormituspiikkejä, ja kaksisuuntaiset palvelutkin ovat lähinnä verkossa täytettäviä lomakkeita.

3.1. Matkaviestinjärjestelmät

Matkaviestinnällä tarkoitetaan tietoliikennettä, jossa käytetään hyväksi ilmatiellä eli radiorajapinnalla vapaasti eteneviä sähkömagneettisia aaltoja. Lisäksi perusajatuksena on se, että radioyhteyttä voidaan käyttää laajalla maantieteellisellä alueella liikkuvien telepäätelaitteiden, kuten kännyköiden, ja televerkkojen välillä [Penttinen, 2006a]. Tässä tutkielmassa keskitytään ensisijaisesti GSM-verkkoihin sekä niistä kehittyneisiin UMTS-verkkoihin. Muut langattomat pääsyteknologiat, kuten WLAN tai WiMAX, jäävät pääsääntöisesti tämän tutkielman ulkopuolelle, koska niitä ei ole yhtä laajamittaisessa käytössä, eivätkä ne muodosta vastaavia vakioituja globaaleja verkkoja.

3.1.1. Standardoidut globaalit digitaaliset solukkoverkot

Nykyaikaisen langattoman viestinnän kulmakivi on solukkoverkko, joka muovautui nykyiseen muotoonsa 1990-luvun alussa Euroopassa. GSM-verkon ja

sitä seuranneen UMTS-verkon komponentit, signalointitekniikka ja rajapinnat on määritelty yhteisten referenssiarkkitehtuurien ja standardien kautta. Verkon määritteli alkujaan operaattoreiden ja laitevalmistajien muodostama järjestö *GSM Association*. Sittemmin verkon teknisten määritysten kehityksestä on vastannut *3GPP*-järjestö (*3rd Generation Partnership Project)*. Vuoden 1999 jälkeen se on julkaissut yhteensä kymmenen versiota määrityskokoelmastaan [3GPP, 2011]. Päivitetyt versiot ovat tuoneet uusia ominaisuuksia niin radioverkon, verkon ytimen kuin palvelujenkin puolelle. Release 99 määritteli ensimmäistä kertaa UMTS-radiorajapinnan, LTE-radioverkko ja EPC-ydin puolestaan tulivat Release 8:ssa vuonna 2008. Yhteisten määritysten ansiosta operaattorit voivat periaatteessa yhdistää verkoissaan usean eri laitevalmistajan tuotteita saumattomasti, joskin valmistajat toki pyrkivät tuomaan vain omien tuotteidensa kanssa yhteensopivia lisätoiminnallisuuksia markkinoille. 3GPP:n ohella toinen merkittävä verkon toimintoja määrittävä taho on vanhempi ja laajemmin toimiva ETSI (*European Telecommunications Standard Institute*), joka julkaisee omina standardeinaan 3GPP:n määritysten lopullisia versioita. Kolmas merkittävä organisaatio on OMA (*Open Mobile Alliance*), joka pyrkii määrittelemään teknologiariippumattomia vakioituja palveluita mobiiliverkkoihin.

Verkon teknisten määritysten versio kuvaa, mitä palveluja ja rajapintoja verkosta löytyy. Monet nykyisin perusominaisuuksiksi mielletyt palvelut, kuten tekstiviestit tai pakettidatayhteydet, eivät olleet mukana alusta alkaen, vaan niitä on lisätty vuosien varrella, ja samalla määrityksistä on julkaistu uusia versioita. Esimerkiksi sijaintiin perustuvat palvelut (Location Services, LCS) tulivat mukaan vasta 3GPP Release 98:ssa, joka julkaistiin alkuvuodesta 1999. Teknisen määrityksen valmistumisesta kuluu vielä aikaa siihen, että laitevalmistajat saavat niitä tukevia uusia tuotteita markkinoille ja operaattorien verkonrakennusta ohjaavat heidän omat markkinastrategiansa sekä taloudelliset realiteetit.

Tässä tutkielmassa tarkastellaan ensisijaisesti toiminnallisuutta, joka on määritelty 3GPP:n standardien versioissa Release 98 – Release 6 (1998 – 2004), sillä uudempien versioiden teknologiaa ei vielä ole laajamittaisesti käytössä tätä kirjoittaessa. Käytännössä verkoissa on käytössä eri osissa eri versioiden mukaista toiminnallisuutta, eikä mikään verkko vastaa täysin yhtä tiettyä versiota. Lisäksi tilaajien omat laitteet vaikuttavat myös verkolta saataviin palveluihin: esimerkiksi jos tilaajan matkapuhelin ei tue kuin perinteistä 2G-tekniikkaa, pitää tarkastelu radioverkon osalta joiltakin osin rajoittaa vain Release 97:n toiminnallisuuksiin. Toisaalta runkoverkko voi tällaisessa tilanteessa kuitenkin tarjota uudempien versioiden palveluita saumattomasti. Kun tutkielmassa myöhemmin viitataan GSM-verkkoon, tarkoitetaan pääsääntöisesti Release

98:ssa määriteltyjä toiminnallisuuksia ja UMTS-verkon osalta puolestaan Release 6:ssa määriteltyjä.

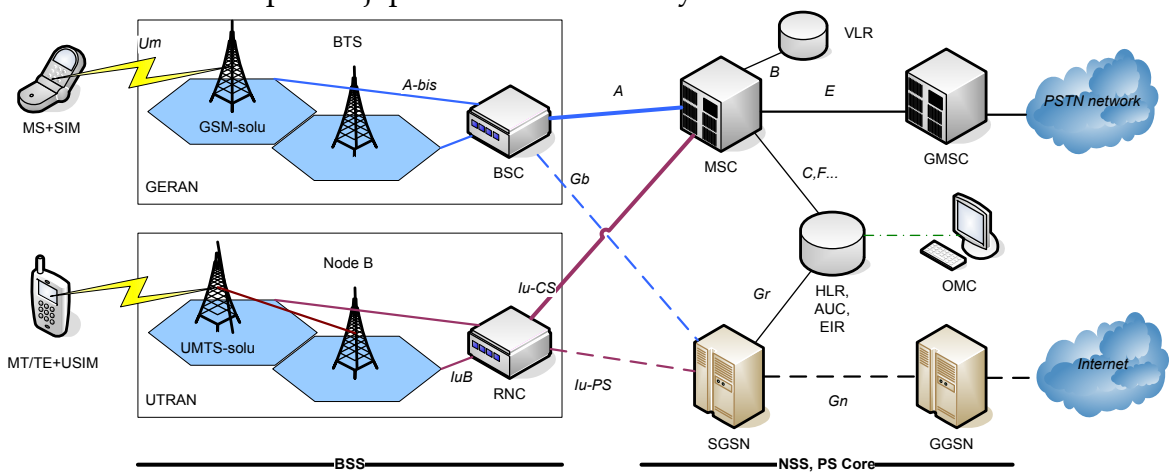
Verkon toiminta on määrityksissä kuvattu yleensä hyvin yksityiskohtaisesti monella eri abstraktiotasolla ns. GSM-protokollapinossa, joka vastaa ISO:n määrittelemän OSI-mallin kerroksia. OSI-mallin kerrokset yhdestä seitsemään ovat: 1. fyysinen kerros; 2. linkkikerros; 3. verkkokerros; 4. kuljetuskerros; 5. istuntokerros; 6. esityskerros ja 7. sovelluskerros [Penttinen, 2006a]. GSM- ja UMTS-verkoissa käytetyt SS7-signalointiprotokollat toimivat yleensä OSI-mallin kolmella alimmalla tasolla sekä sovellustasolla.

3.1.2. GSM- ja UMTS-verkkojen arkkitehtuuri

Mobiiliverkon sukupolvesta riippumatta sen arkkitehtuuri voidaan perustasolla jakaa karkeasti seuraaviin osiin:

- Käyttäjän päätelaite (*MS, Mobile Station)* ja siinä oleva tunnistusmoduuli (SIM-kortti).
- Radioverkon laitteisto, eli yleispuheessa tukiasemat, tarkemmin myös tukiasemaohjaimet (*BSS, Base Station Subsystem)*.
- Siirtoverkko tukiasemien, tukiasemaohjainten ja verkon ytimen välillä- Verkon ydin (*NSS, Network Switching Subsystem*) eli matkapuhelinkeskukset (MSC) sekä pakettidataverkon elementit.
- Ytimeen yhteydessä olevat erilaiset rekisteripalvelut (HLR, VLR ym.) sekä käytönhallintajärjestelmät [Penttinen, 2006a].

GSM-verkon yleinen arkkitehtuuri on määritelty 3GPP:n ja ETSI:n teknisessä dokumentissa [ETSI, 2000]. Yksinkertaistettu GSM- ja UMTS-verkkojen arkkitehtuuri tärkeimpine rajapintoineen on esitetty kuvassa 3.



Kuva 3. GSM- ja UMTS-verkkojen keskeiset elementit ja rajapinnat

Operaattorin matkaviestinverkosta on myös yhteydet muihin verkkoihin, kuten toisiin matkaviestinverkkoihin, yleiseen puhelinverkkoon sekä Internetiin. Palvelujen lisääntyessä myös verkot ovat monimutkaistuneet, sillä uudet palvelut on usein ollut mahdollista toteuttaa modulaarisesti tuomalla verkkoon uusia verkkoelementtejä. Toisaalta teknologian kehittyessä monista lisäominaisuuksista on tullut peruselementteihin integroituja vakiotoimintoja. 3GPP on myös pyrkinyt aktiivisesti yksinkertaistamaan ja selkeyttämään verkon arkkitehtuuria teknologian kehittyessä mm. siirtymällä täysin IP-pohjaiseen liikennöintiin runkoverkon tasolla.

Tukiasemajärjestelmä (BSS) hoitaa radioliikennettä ja radioresurssien hallintaa päätelaitteiden ja verkon välillä. Tukiasemat ovat yksinkertaisimmillaan radiolähettimiä ja -vastaanottimia, jotka palvelevat aina tiettyä määrättyä maantieteellistä aluetta omalla kutsutaajuudellaan. Tätä yhden tukiaseman aluetta kutsutaan *soluksi* (engl. *cell*). Solujen koko vaihtelee muutamista kymmenistä metreistä (esimerkiksi kauppakeskusten sisätilat) kymmeniin kilometreihin (haja-asutusalue). Solujen kuuluvuusalueet menevät reunoiltaan päällekkäin, jolloin päätelaite voi joustavasti vaihtaa tukiasemasta toiseen ilman, että aktiivinen puhelu tai datayhteys katkeaa. Yhteyttä voidaan vaihtaa myös eri radioverkkotekniikoiden (GSM, EDGE, WCDMA, UMTS-TDD) välillä tarpeen ja kuuluvuuden mukaan. Joukkoa tukiasemia hallitsee tukiasemaohjain (BSC, *Base Station Controller*, tai UMTS-verkoissa RNC, *Radio Network Controller*). Tukiasemajärjestelmästä ja radioverkosta voidaan käyttää myös yleisnimitystä RAN (Radio Access Network).

Siirtoverkon yhteydet tukiasemien ja tukiasemaohjainten sekä edelleen tukiasemaohjaimilta eteenpäin verkon ytimeen voidaan toteuttaa monin eri tavoin. GSM-verkossa yksittäinen tukiasema voi toimia vain 2 Mbit/s E1-yhteyden varassa (*A-bis*-rajapinta), mutta käyttäjämäärän sekä ennen kaikkea pakettidataliikenteen kasvaessa yhteydet toteutetaan nykyään yhä useammin nopeammin valokuitu- tai radiolinkkiyhteyksin. Verkkotekniikan kehityksen myötä uudemmissa verkoissa on myös mahdollista toteuttaa siirtoyhteyksiä IP-verkkojen päällä, mikä yksinkertaistaa ja harmonisoi niitä operaattoreiden muiden verkkojen kanssa.

Verkon ydin (CN, Core Network) pitää sisällään piirikytkentäisen keskusjärjestelmän (NSS, *Network Switching Subsystem*) sekä pakettidatayhteyksien osalta oman, osittain erillisen pakettikytkentäisen ytimen. Keskusjärjestelmän tärkeimmät elementit ovat matkapuhelinkeskukset (MSC, *Mobile Switching Center*) sekä niihin liittyvät rekisterit, joista tärkeimmät ovat kotirekisteri (HLR, *Home Location Register*), vierailijarekisteri (VLR, *Visitor Location Register*), tunnistuskeskus (AuC, *Authentication Center*) sekä laitetunnusrekisteri (EIR, *Equipment*

Identification Register). Kotirekisterissä ylläpidetään tietoja verkossa olevista liittymistä ja niiden palveluista. Vierailijarekisterissä, joka on yleensä integroitu matkapuhelinkeskukseen, pidetään tietoja kyseisen rekisterin/keskuksen toimialueella kulloinkin olevista liittymistä [ETSI, 2000].

3.1.3. Mobiliteetin hallinta GSM/UMTS-verkossa

Matkanviestinverkon yksi tärkeimpiä käyttäjiä tukevia tehtäviä on liikkuvuuden eli mobiliteetin hallinta, joka mahdollistaa sen, että liikkuva käyttäjä on aina tavoitettavissa ja toisaalta tämä pystyy muodostamaan yhteyksiä samaan tapaan sijainnista riippumatta. Mobiliteetin hallintaan liittyy kaksi perusongelmaa: sijainnin hallinta, eli käyttäjän liikkeiden seuraaminen verkossa, ja toisena handover-toiminnallisuus, joka mahdollistaa aktiivisen yhteyden säilymisen käyttäjän liikkuessa toiselle alueelle verkossa. [Razavi, 2011].

Matkaviestinverkoissa välitettävä liikenne voidaan jakaa kolmeen erilliseen päätyyppiin: äänipuheluille varatut piirikytkentäiset yhteydet, pakettidatayhteydet sekä verkon toiminnan ja yhteyksien kontrollointiin käytetty signalointi. GSM-verkoissa signalointi perustuu kiinteän puhelinverkon SS7-signalointiin, johon on tehty matkaviestinverkkoja varten erinäisiä laajennuksia, tärkeimpänä päätelaitteiden liikkuvuuden eli mobiliteetin hallinta. GSM-signaloinnin protokollapinossa kolmas taso jakautuu edelleen kolmeen alitasoon, joita ovat radioresurssien hallinta (RR, *Radio Resource management*), liikkuvuuden hallinta (MM, *Mobility Management*) sekä yhteyksien hallinta (CM, *Connection Management*). Kun päätelaite on rekisteröitynyt verkkoon ja verkko on autentikoinut päätelaitteen hyväksytysti, päätelaite valitsee kuuluvuusalueellaan olevista valitun verkon soluista yhden ja jää kuuntelemaan solun kutsukanavaa.

Sijainnin hallinta GSM- ja UMTS-verkoissa perustuu siihen, että verkko tietää normaalisti päätelaitteiden sijainnin vain summittaisesti verkkoon määritellyn *sijaintialueen (*LA, *Location Area*) tarkkuudella. LA on operaattorin määrittelemä joukko soluja, jotka voivat teknisesti sijaita mielivaltaisella maantieteellisellä alueella. Yleensä LA:t kuitenkin muodostavat yhtenäisiä maantieteellisiä kokonaisuuksia. Yhden LA:n alueella voi olla yksi tai useampia tukiasemaohjaimia (BSC), jotka huolehtivat radioresurssien allokoinnista soluissa. Valmiustilassa oleva päätelaite ei normaalisti päivitä sijaintiaan verkolle muuta kuin silloin, kun se liikkuu toisen LA:n alueella olevalle solulle.

Tukiasemaohjaimia ja niihin assosioitua LA-joukkoa puolestaan ohjaa matkapuhelinkeskus (MSC) ja siihen liitetty vierailijarekisteri (VLR), joka pitää kirjaa kaikista alueellaan olevista päätelaitteista ja niiden sijainnista LA:n tarkkuudella. Saapuvan puhelun (tai tekstiviestin, jos käyttäjällä ei ole aktiivista datayhteyttä) tapauksessa verkko selvittää VLR:stä, minkä LA:n alueella päätelai-

te pitäisi olla. Tämän jälkeen lähetetään kaikille alueen tukiasemaohjaimille ja edelleen tukiasemille kutsu päätelaitteelle solujen kutsukanavilla. Vasta päätelaitteen kuullessa ja vastatessa sille osoitetun kutsun verkko tietää tarkasti, minkä solun alueella päätelaite on ja muodostaa varsinaisen yhteyden. [Penttinen, 2006a]

Sijaintialueiden koolla ja määrällä on merkittävä vaikutus verkossa tapahtuvaan signalointiin, mikä osaltaan vaatii kapasiteettia niin transmissioverkolta kuin verkon aktiivikomponenteiltakin. Suurimmillaan LA voisi olla koko MSC/VLR-alueen kokoinen, mutta tällöin saapuvien puheluiden kohdalla päätelaitetta paikannettaessa pitäisi lähettää signalointia koko verkon alueelle. Vastaavasti pienimmillään LA voisi olla vain solun kokoinen, mutta tästä taas seuraisi runsaasti signalointia päätelaitteiden liikkuessa verkossa ja päivittäessä sijaintiaan. Operaattori voi myös pakottaa päätelaitteet lähettämään säännöllisin väliajoin sijaintipäivityksiä, vaikka ne eivät LA:ta vaihtaisikaan, mutta tästä seuraa huomattava signalointikuorma, eikä ominaisuutta sen vuoksi juurikaan käytetä.

3G-verkoissa (UMTS) toteutus on pääosin GSM-verkkoja vastaava. Sijaintialueen tilalla käytetään usein ilmausta *palvelualue (*SA, *Service Area*). Yhtenä UMTS:n keskeisenä erona GSM:ään on kahden radioverkko-ohjaimen välinen suora Iur-rajapinta, jolloin signalointi ei kuormita runkoverkkoa yhtä paljoa kuin GSM:n tapauksessa. Verkko ei kuitenkaan lähtökohtaisesti edelleenkään tiedä valmiustilassa olevan päätelaitteen sijaintia sen tarkemmin, ellei käytössä ole erillisiä sijaintipalveluita. Pakettikytkentäisen liikenteen osalta LA:n rinnalla toimii käsite *reititysalue* (RA, *Routing Area*), joka tarkoittaa aluetta, jolla päätelaite voi liikkua ilman sitä palvelevan GPRS-noodin (SGSN:n) vaihtamista.

3.1.4. Mobiiliverkkojen evoluutio

Toisen ja kolmannen sukupolven GSM/UTMS-verkkoja seuraavat uudemmat teknologiat. Näistä neljännen sukupolven verkkotekniikoista matkaviestinverkoissa keskeisin on LTE (*Long Term Evolution*) radioverkkojen puolella ja siihen liittyvä EPC (*Enhanced Packet Core*). Verkot muuttuvat yhä hybridimäisemmäksi erilaisten pääsyteknologioiden, kuten WLANin myötä. Päätelaitteiden käyttö muuttuu myös merkittävästi aiemmasta puhe- ja tekstiviestikäytöstä yhä kasvavissa määrin datakäyttöön. LTE-verkossa ei ole enää lainkaan piirikytkentäisiä yhteyksiä perinteisen puheyhteyden välittämiseen, vaan kaikki liikenne kulkee pakettikytkentäisenä IP:n päällä.

LTE-verkoissa on myös kehitetty mobiliteetin hallintaa aiempiin teknologioihin verrattuna. Joukko LTE-verkon soluja muodostaa *jäljitysalueen* (TA,

Tracking Area), joka vastaa GSM- ja UMTS-verkon sijainti- tai palvelualuetta. LTE-verkoissa on pyritty aiempia teknologoita helpompaan muunneltavuuteen, jonka ansiosta verkko voi joustavammin mukautua erilaisiin käyttötilanteisiin. 3GPP:n Release 8 toi mukanaan käsitteen jäljitysaluelista (TAL, *Tracking Area List*). Sen myötä jokaiselle päätelaitteelle voidaan määrittää useammasta TA:sta koostuva joukko, jossa nämä voivat liikkua ilman sijaintitiedon päivitystä verkolle [Razavi, 2011].

Tutkielman kannalta olennainen päätelaitteiden paikantaminen vaihtelee teknologioittain. Useimmat 3GPP:n standardoimat paikannusmenetelmät siirtynevät luontevasti myös neljännen sukupolven matkaviestinverkkoihin, ja verkon näkökulmasta paikantaminen todennäköisesti tulee toimimaan vähintään yhtä hyvin kuin nykyisissä verkoissa. Sen sijaan vaihtoehtoisten pääsyverkkojen, kuten kolmansien osapuolten WLAN-hotspottien, käyttö tuo mukanaan omat haasteensa. Tällöin paikantamisessa korostuu päätelaitteen itse tekemä GPS-pohjainen paikannus, verkon puolelta vastaavaan yhtenäistettyyn paikantamiseen tuskin tullaan pääsemään.

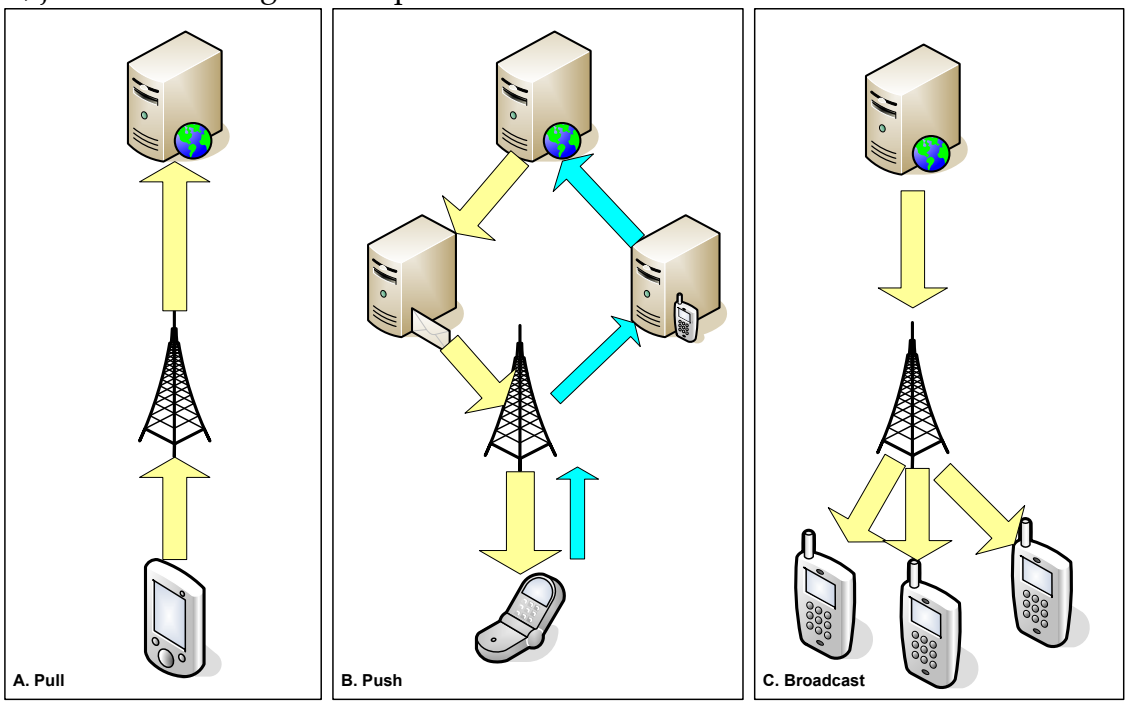
3.2. Sijaintipohjaiset palvelut mobiiliverkoissa

Sijaintipohjaiset palvelut (LBS, *Location-based Services*) tarkoittavat mobiiliverkossa joko päätelaitteen käyttäjälle, verkolle tai kolmansille osapuolille tarjottavia palveluita, jotka hyödyntävät tietoa päätelaitteen sijainnista.

Aloudat ja Michael [2011] jakavat sijaintipohjaiset palvelut kahteen ryhmään: reaktiivisiin (pull) ja proaktiivisiin (push). Reaktiiviset palvelut vaativat aina käyttäjän toimenpidettä, jotta päätelaite hakee sijaintitietoon perustuvaa informaatiota. Vastaavasti proaktiiviset palvelut käynnistyvät automaattisesti heti, kun ennalta määritelty sijaintitietoon perustuva asia tapahtuu, esimerkiksi käyttäjä saapuu tai poistuu tietyltä alueelta. Valtaosa tämän päivän toteutetuista sijaintipohjaisista palveluista perustuu reaktiiviseen pull-malliin. Tällaisia ovat esimerkiksi puhelinten karttasovellukset, jotka hakevat sijainnin perusteella verkosta lisätietoa lähistöllä olevista kohteista. Proaktiiviset palvelut ovat yleensä huomattavasti raskaampia toteuttaa, koska ne vaativat verkolta päätelaitteen sijainnin seuraamista. Esimerkiksi vaaratiedotteiden välitysjärjestelmän näkökulmasta tällainen edellyttää verkolta merkittäviä resursseja.

Tarkasteltaessa sijainnin perusteella lähetettäviä viestejä verkon käyttäjille, voidaan erottaa pull- ja push-palvelujen rinnalle vielä kolmas vaihtoehto. Broadcast-mallissa hyödynnetään verkon fyysistä topologiaa ja lähetetään viesti kaikille tiettyjen tukiasemien alueella oleville päätelaitteille (ks. Kuva 4). Tällainen palvelumuoto on reaktiivisiin tai proaktiivisiin verrattuna passiivinen,

sillä se ei vaadi päätelaitteelta eikä verkolta erillisiä toimenpiteitä, vaan viesti välittyy automaattisesti kaikille tukiaseman kuuluvuusalueella oleville laitteille, joiden tulisi reagoida saapuvaan viestiin automaattisesti.



Kuva 4. Sijaintipohjaisten palveluiden jaottelu

3.2.1. Päätelaitteen itse tekemä paikannus

Modernit päätelaitteet voivat selvittää oman sijaintinsa monin eri tavoin. Yksinkertaisimmillaan ne tietävät aktiivisen solun tunnistenumeron ja voivat tätä vasten selvittää joko puhelimen muistissa olevasta tai Internet-yhteydellä tavoitettavasta tietokannasta maakoodia, operaattorikoodia ja solunumeroa vastaavan sijaintitiedon. Päätelaite voi edelleen tarkentaa sijaintipäätelmää vastaanottamiensa solujen radiosignaalien voimakkuuden perusteella trianguloroimalla. Älypuhelinten karttasovellukset, kuten Google Maps tai Nokia Ovi (tai nykyään yleensä älypuhelimen käyttöjärjestelmään liitetty sijaintipalvelu), käyttävätkin tätä verkkopohjaista paikannusta, mikäli tarkempaa paikkatietoa ei ole saatavilla. Nykyään lähes poikkeuksetta kaikissa älypuhelimissa on GPS-vastaanotin, joka pystyy sekunneissa paikantamaan puhelimen sijainnin muutaman metrin tarkkuudella ulkotilassa. Sijaintitiedon hyödyntäminen on vakioitu älypuhelinten omien ohjelmistokirjastojen lisäksi mm. HTML5:n Geolocation API:ssa, jonka myötä sijainti voidaan selvittää WWW-selaimessa suoritettavan JavaScript-koodinkin avulla. Sijaintipohjaiset palvelut lisääntyvät jatkuvasti mobiilisovelluksissa. Esimerkiksi www-sivuilla esitettävät mainokset ovat yhä useammin optimoitu käyttäjän sijainnin mukaan ja sijaintietoa hyödynne-

tään myös lukuisissa peleissä. Vaikka älypuhelinten sovellukset tarvitsevatkin asennuksen yhteydessä erikseen luvan sijaintitiedon käyttämiseen, monet käyttäjät yleensä valitsevat tämän, sillä se saattaa olla jopa edellytyksenä sovelluksen asentamiselle.

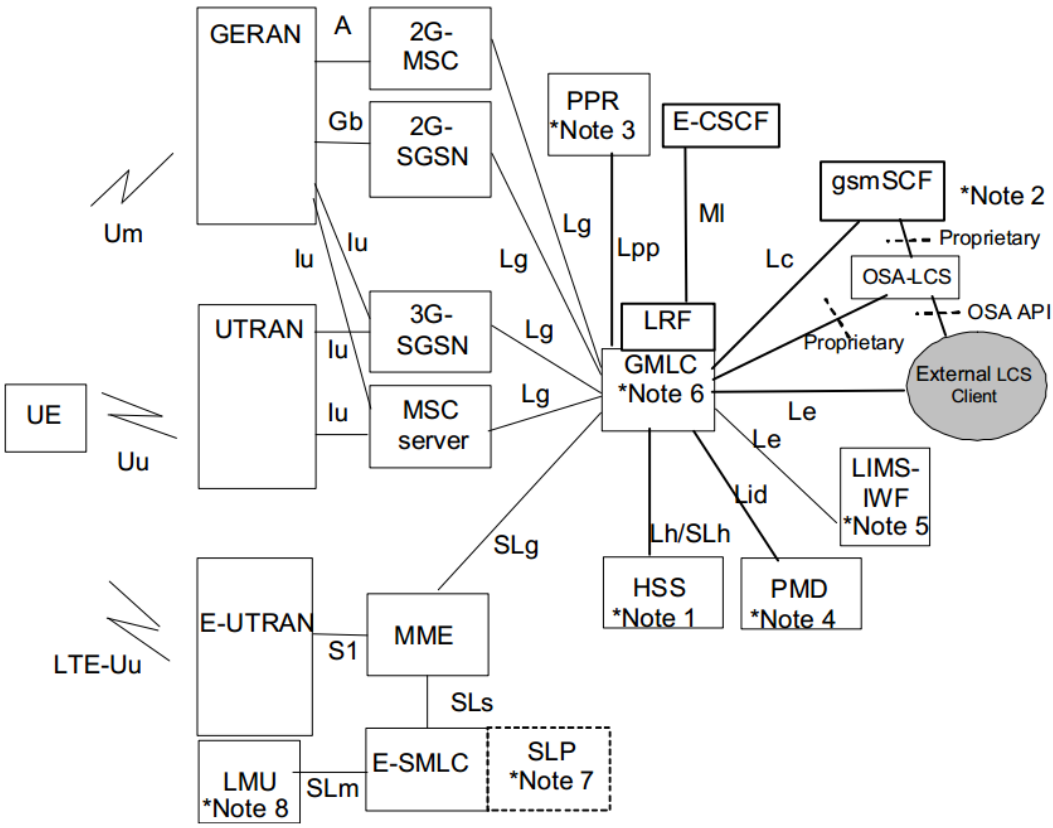
3.2.2. Verkkopohjainen paikannus

Verkkopohjaisessa paikantamisessa aloite päätelaitteen sijainnin selvittämiseen tulee verkon suunnalta. Kun paikannus tapahtuu kokonaan verkon hallintatasolla, se on päätelaitteen kannalta passiivinen operaatio. Paikannus voidaan myös tehdä hybridimenetelmällä, jossa verkko kysyy päätelaitteelta mahdollista tarkempaa sijaintia laitteen itse suorittaman paikannuksen (yleensä GPS) perusteella. Menetelmät soveltuvat kohtuullisesti yksittäisen päätelaitteen paikantamiseen, mutta tällöin paikantamisavaimena on lähtökohtaisesti aina päätelaitteen liittymän tilaajanumero (MSISDN). Verkkopohjaisessa paikantamisessa haasteena on kuitenkin useiden tilaajien paikantaminen. Koska paikantamisen hakuavaimena on aina tilaajan tai SIM-kortin numero, pitäisi tietyllä alueella olevien tilaajien selvittämiseksi käytännössä paikantaa kaikki verkossa olevat tilaajat eli Suomen operaattoreiden tapauksessa useita miljoonia liittymiä. Kuten Ficek ja muut [2010] toteavat, verkko ei normaalisti automaattisesti ylläpidä ajantasaista sijaintietoa, vaan jokaisen liittymän sijainti on selvitettävä erillisellä kyselyllä. Verkkopohjaisen massapaikantamisen ongelmia käsittelen tarkemmin alakohdassa 3.3.1.

Verkkopohjainen paikannuspalvelu (LCS) on standardoitu ETSIn ja 3GPP:n teknisissä määrityksissä alkujaan GSM-verkoille ja edelleen laajennettu ja päivitetty UMTS- ja LTE-verkoille [ETSI, 2013a]. Mikäli pääsyverkko kykenee paikantamaan päätelaitteita, sen tulisi kyetä kommunikoimaan sijaintitiedot edelleen muulle verkolle LCS-määrityksen mukaisesti. LCS-määrityksessä verkkoon luodaan uusia loogisia verkkoelementtejä (olennaisimpana LCS-palvelin ja GMLC, *Gateway Mobile Location Center*), jotka tarjoavat varsinaisesta verkon signaloinnista ja liikenteenvälityksestä erillisiä paikannuspalveluita sekä päätelaitteille että verkkoon liitetyille ulkoisille LCS-asiakkaille (esimerkiksi hätäkeskuksen tietojärjestelmä). LCS:n verkkoelementtien liittyminen erityyppisiin mobiiliverkkoihin on esitetty kuvassa 5. Verkko itsessään voi myös hyödyntää sijaintitietoja esimerkiksi sijaintiperustaisessa laskutuksessa. ETSIn määritys on tehty kattamaan kaikenlaisten sijaintipohjaisten palvelujen tarjoaminen, joten siinä on huomioitu myös erilaiset yksityisyysvaatimukset, sijaintihakujen laskutus ja sijaintihaun laatu (QoS). Näillä ominaisuuksilla ei kuitenkaan ole merkitystä hätäpaikannuksen kannalta, mutta ne mahdollistavat erilaiset lisäarvo-

palvelut (ks. alakohta 3.2.3). Määritys jakaa sijaintipalvelut neljään eri kategoriaan:

- kaupalliset (lisäarvopalvelut)
- sisäiset (pääsyverkon omat toiminnot)
- hätäpuhelut (hätäpuhelun automaattinen paikannus, toteutus Suomessa kuvattu tarkemmin alakohdassa 3.2.4)
- viranomaispaikannus (esim. poliisin suorittama epäillyn seuranta).



Kuva 5. LCS:n yleiskuvaus [ETSI, 2013a]

LCS-määritys olettaa, että varsinaiset päätelaitteen paikannusteknologiat ovat spesifisiä eri pääsyverkoille. Esimerkiksi UMTS- ja LTE-verkoissa voidaan käyttää huomattavasti kehittyneempiä ja tarkempia radioverkon paikannusmenetelmiä kuin perinteisessä toisen sukupolven GSM-verkossa. LCS-palvelimen tulisi tukea myös päätelaitteen jatkuvaa seurantaa, jolloin se raportoi LCS-asiakkaan kysymän laitteen sijaintitiedot määräajoin. Käytännössä jatkuva seuranta aiheuttaa verkkoon huomattavaa signalointikuormaa, eikä se siksi sovellu käytettäväksi laajamittaisesti. Kuormitusta voidaan vähentää hyväksymällä jatkuvissa päivityksissä suurempi toleranssi, jolloin tarkkaa paikannusta ei suoriteta jokaisella päivityskerralla, vaan raportoidaan vain viimeisin tiedetty sijainti.

3.2.3. Sijaintitietoon perustuvat palvelut ja yksityisyydensuoja

Useimmat nykyisistä älypuhelinsovelluksista hyödyntävät sijaintitietoa. Ilmeisimpiä esimerkkejä ovat erilaiset karttapalvelut kuten Google Maps, jotka näyttävät käyttäjän sijainnin ja osaavat etsiä sen perusteella lähistöllä olevia palveluita tai tarjota reittiohjeita. Myös erilaiset kuntoilusovellukset hyödyntävät paikkatietoa laskien esimerkiksi juoksulenkin aikana kulutettua kalorimäärää huomioiden reitin nousut ja laskut. Useat sosiaalisen median sovellukset hyödyntävät sijaintitietoa ja tarjoavat käyttäjälle aktiivisesti mahdollisuutta merkitä oma sijainti jaettaviin päivityksiin ja valokuviin.

Käyttäjän sijainnin jakaminen muille on aina lähtökohtaisesti arveluttavaa yksityisyyden näkökulmasta, ja tätä säädelläänkin melko tiukasti Suomen lainsäädännössä. Verkkoon sijaintitietoa päivittävä sovellus tai verkkopohjainen paikannus mahdollistaa teknisesti käyttäjän paikantamisen myös tämän tietämättä. Suomessa esimerkiksi käyttäjän sijainnin paikantamisesta hätätilanteessa on melko tarkasti säädetty laissa [Viestintävirasto, 2004]. Myös sellaiset sovellukset kuten vankien lomien ja koevapauksien seurantaan käytetyt sijaintietietoa lähettävät jalkapannat edellyttävät aina valvottavan itsensä suostumuksen. Teleoperaattorit ovat aiemmin tarjonneet palveluita, joissa käyttäjä voi itse jakaa sijaintitietonsa valitsemilleen henkilöille, esim. lähiomaisille, mutta näistä luovuttiin vähäisen kysynnän ja yksityisyydensuojaan liittyvien ongelmien vuoksi [YLE, 2009].

Monissa muissa maissa yksityisyydensuoja ei välttämättä kuitenkaan ole samalla tasolla kuin Suomessa, varsinkaan sellaisissa tilanteissa, joissa vallitseva hallinto kokee asemansa uhatuksi. Useassa sisäisesti epävakaassa valtiossa onkin esitetty väitteitä siitä, että vallassa olevat viranomaiset ovat hyödyntäneet puhelinten sijaintitietoja hallitusta vastustavien mielenosoittajien tunnistamisessa [Guardian, 2014]. Viime aikoina on myös herännyt epäilyjä siitä, ovatko käyttäjien erilaisiin pilvipalveluihin (Facebook tai Google) tallentamat tiedot suojassa ulkomaisilta tiedusteluviranomaisilta.

3.2.4. Päätelaitteen sijainnin paikallistaminen hätätilanteessa

Nykyisellään Suomessa hätäkeskukset käyttävät mobiilipaikannusta puhelinten hätäpaikannukseen (Emergency Positioning). Puhelimen sijainti paikantamalla voidaan helpottaa avun ohjausta kohteeseen, jos soittaja ei tiedä tai pysty itse ilmaisemaan tarkkaa sijaintiaan. Hätäpaikantamisen toteuttamisesta on säädetty Euroopan Unionin E112 -direktiivissä (2003), joka puolestaan pohjau-

tuu sisällöllisesti pitkälti yhdysvaltalaiseen Federal Communication Commissionin E911 -säädökseen. Suomen lainsäädännössä asiasta on säädetty Hätäkeskuslaissa (18.2.2000/157 ja muutos 16.6.2004/519), Sähköisen viestinnän tietosuojalaissa (16.6.2004/516) sekä Viestintämarkkinalaissa (23.5.2003/393). Viestintävirasto [2004] asetti paikannuksen tarkkuuden vaatimukseksi operaattoreille saman, jota kaupallisissa paikannuspalveluissa tarjotaan. Automaattiset järjestelmät hätäpuheluiden paikantamiseen hätäkeskuksista otettiin laajamittaiseen käyttöön vuoden 2005 aikana, jonka jälkeen puhelut on saatu paikannettua noin 10 sekunnissa.

Hätäpaikannuksen tekeminen edellyttää lain mukaan aina perusteltua olettamaa hätäpaikannuksen kohteena olevan henkilön olemisesta akuutissa hengen tai terveyden vaarassa. Hätäkeskus voi siis harkintansa mukaan paikantaa järjestelmän kautta joko sen liittymän, josta hätäilmoitus on tehty, tai hätäilmoituksen kohteena olevan henkilön liittymän, jos kyseinen henkilö on hätäilmoituksen vastaanottaneen hätäkeskuspäivystäjän perustellun käsityksen mukaan ilmeisesti hädässä tai välittömässä vaarassa. Paikannusta ei ole oikeutettua kuitenkaan käyttää esimerkiksi rikoksen estämiseksi tai selvittämiseksi [Hätäkeskuslaitos, 2010].

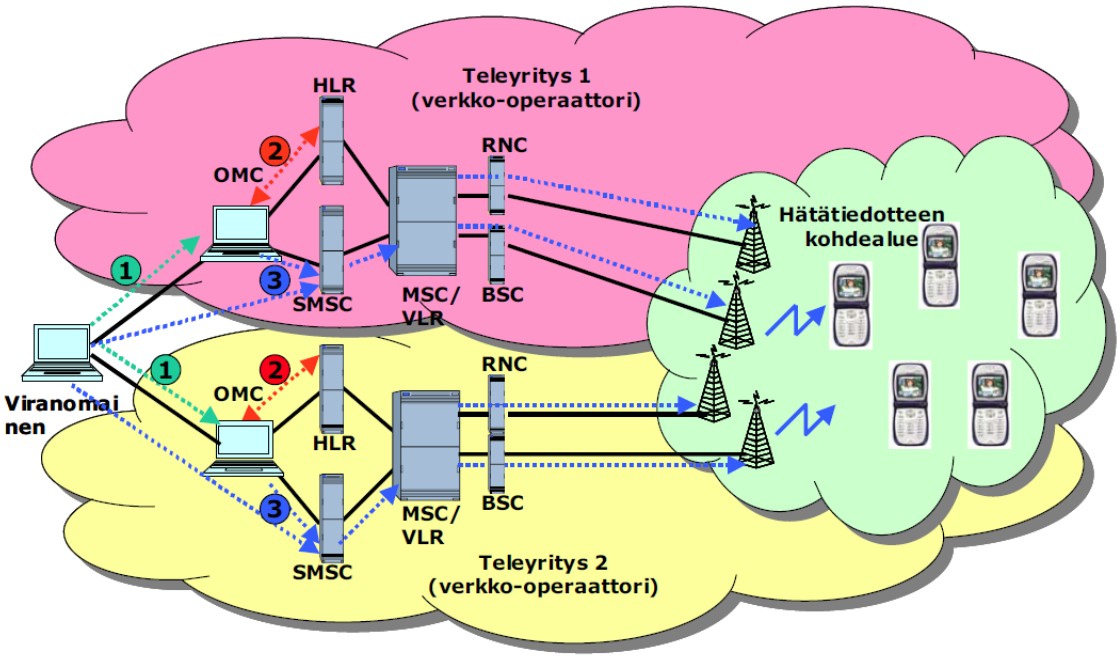
Hätäkeskukset paikantavat hätäpuhelun vakioidun Mobile Location Protocolin (MLP) avulla. MLP on sovellustasoinen protokolla, joka on tarkoitettu päätelaitteen sijainnin selvittämiseen verkon toteutusteknologiasta riippumatta [OMA, 2010]. Suomen teleoperaattoreiden yhteistyöfoorumi FiCom on tehnyt oman kansallisen sovelluksen, joka on merkittäviltä osin yhteensopiva MLP:n kanssa. Paikannustieto saadaan automaattisesti parissa sekunnissa liittymän kotiverkko-operaattorin paikannuspalvelimelta (GMLC). Järjestelmä ei kuitenkaan tue ulkomaisten liittymien (roaming) eikä SIM-kortittomien puhelinten paikannusta. Varajärjestelmänä on paikannustiedon kysely operaattorin päivystäjältä telefaxilla. Hätäpaikannus ei kuitenkaan ole aukotonta. Paikantaminen voi olla verkkoalueesta riippuen hyvinkin epätarkkaa tai joissakin tilanteissa epäonnistua kokonaan. Yksittäisen päätelaitteen hätäpaikantamiseen liittyvät ongelmat pätevät osin myös useiden päätelaitteiden paikantamiseen, joskin käyttötarkoituksen ollessa tietyllä alueella olevien paikantaminen riittää yleensä pienempi tarkkuus kuin yksittäistä liittymää paikannettaessa [Rönkkö, 2008].

Automaattisen hätäpaikantamisen yhtenä merkittävänä sovelluksena on automaattinen liikenneonnettomuuksien ilmoitusjärjestelmä, jossa ajoneuvoihin asennettavat laitteet ilmoittavat itsenäisesti sensoritiedon perusteella onnettomuudesta hätäkeskukseen. Järjestelmän uskotaan parantavan merkittävästi pelastusviranomaisten vasteaikaa liikenneonnettomuuksissa ja vähentävän siten tieliikennekuolemia. EU:n eCall-hanke tähtää koko Euroopan laajuiseen

standardoituun järjestelmään, joka otettaisiin käyttöön 2015. Järjestelmän arvioidaan vähentävän liikennekuolemia jopa 2500:llä vuodessa EU:n alueella [VTT, 2009].

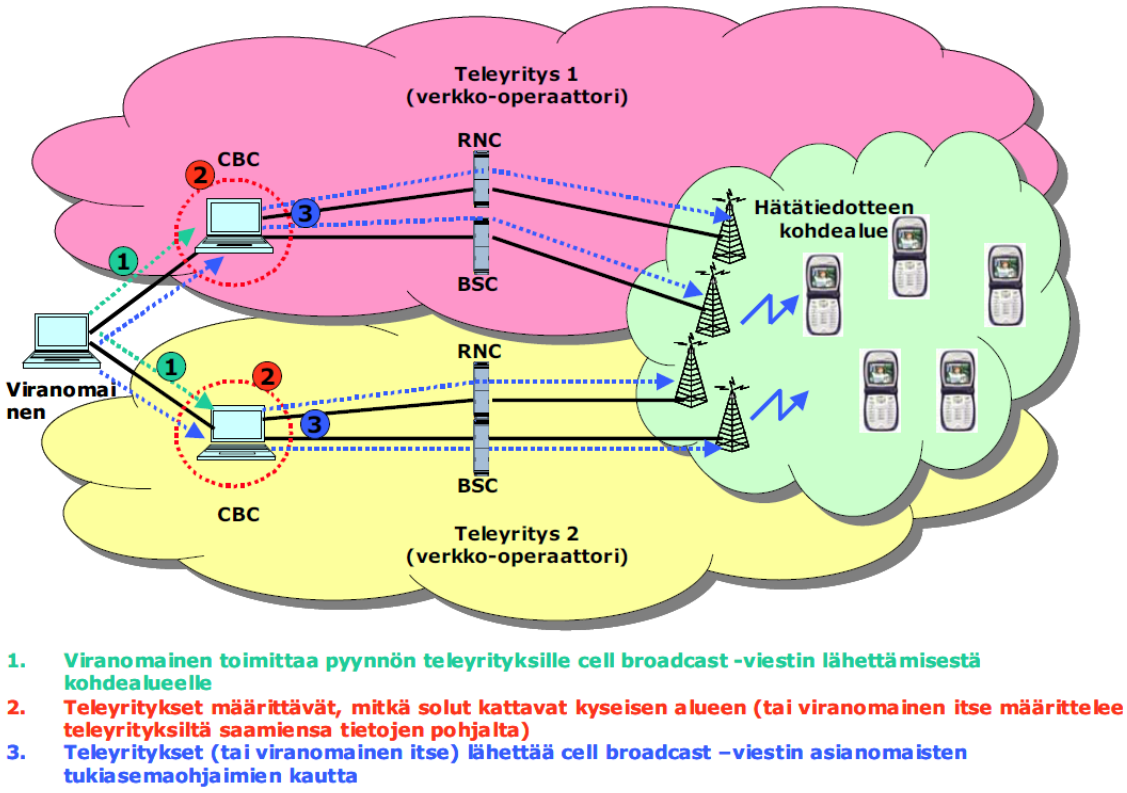
3.3. Alueellisesti kohdennettujen tiedotteiden välittäminen

Alueellisesti kohdennetut vaaratiedoteviestit voidaan välittää mobiiliverkon laitteisiin tekstiviesteinä pääsääntöisesti kahdella eri menetelmällä: normaalit tekstiviestit (SMS, kuva 6) ja soluyleislähetys (CBS, kuva 7). Normaaleihin tekstiviesteihin perustuvan järjestelmän ilmeinen etu on, että sen avulla lähetetty hätätiedote voidaan vastaanottaa kaikissa matkaviestimissä ilman erityisiä toimenpiteitä.



Kuva 6. SMS-järjestelmän toimintaperiaate [Viestintävirasto, 2005]

Ongelmana on kuitenkin järjestelmän kuluttama aika, joka kasvaa sitä pidemmäksi, mitä suuremmalle joukolle hätätiedote lähetetään. Tämä johtuu kaksivaiheisesta toiminnasta, jossa ensin selvitetään kohdealueella olevat liittymät ja sen jälkeen jokaiseen lähetetään yksitellen varoitustekstiviesti. Normaali tekstiviesti tarvitsee aina vastaanottajan liittymän numeron viestin toimittamista varten, joten ennen kuin viestejä voidaan lähettää, on selvitettävä alueella olevat liittymät. Tähän liittyviä ongelmia kuvaan tarkemmin seuraavassa alakohdassa.



Kuva 7. CBS-järjestelmän toimintaperiaate [Viestintävirasto, 2005]

CBS-järjestelmässä viestien lähettäminen on huomattavasti nopeampaa, koska siinä tilaajia ei tarvitse erikseen paikantaa, vaan kaikki kohdealueen kattavien solujen alueella olevat matkaviestimet vastaanottavat viestin, mikäli ne ovat erikseen etukäteen asetettu CBS-viestien vastaanottotilaan [Viestintävirasto, 2005]. Molemmat ratkaisut toimivat vain yhden operaattorin liittymiin, joten valittu teknologia tulisi joka tapauksessa toteuttaa kaikkien operaattoreiden verkoissa, ja viestit lähettävällä viranomaisella tulisi olla yhteys kaikkien verkko-operaattoreiden järjestelmiin viestien toimittamiseksi.

3.3.1. Päätelaitteiden paikantamisen haasteet

Mobiiliverkossa voidaan päätelaitteiden sijaintia tarkastella verkon näkökulmasta SMS-lähetystä silmällä pitäen kolmella eri tarkkuustasolla (esimerkit ja alueet Suomesta):

1. VLR-tarkkuus. Alueita neljästä kymmeneen operaattorista riippuen, maantieteellisesti n. puolesta kahteen lääniä.
2. LA/SA-tarkkuus. Alueita 40-150 operaattorista riippuen. Alueen koko vaihtelee, Etelä-Suomessa halkaisija n. 20 km, Keski-Suomessa 20-100 km, Pohjois-Suomessa yli 100 km (maksimissaan yksi LA kattaa koko Pohjois-Suomen)

3. Solun tarkkuus. 10 000 – 20 000 kpl operaattorista riippuen, alueen halkaisija 100 m – 20 km.

Ulkomaille lähetettävissä vaaratiedotteissa tarkkuutena on aina koko kohdemaa, sillä operaattoreilla ei ole tietoja vieraiden verkkojen maantieteellisestä toteutuksesta.

Vaaratiedotteiden kohdalla lähtökohtana on, että viestien meno hieman aiottua suuremmalle kohdejoukolle ei ole haitallista. Operaattoreilla on omissa verkkotietojärjestelmissään tieto solujen sijainneista, mutta tiedot eivät välttämättä ole suoraan hyödynnettävässä muodossa. Matkaviestinverkossa käytettävien teknisten tunnusten ja hätäkeskuksen käyttämien vaaratiedotteiden kohdealueen määrittelevien alueiden vastaavuus tuleekin määrittää operaattorikohtaisesti [Viestintävirasto, 2005].

Liittymien paikannus ei myöskään toimi samalla tavalla kaikkien teleyritysten kohdalla johtuen verkkotekniikan eroista. Viestintävirasto on arvioinut, että karkeasti verkkotekniikasta ja sen toimittajasta riippumatta VLR-tarkkuudella liittymien haku kestäisi toimintatavasta riippuen n. 30 min – 8 h johtuen tilaajien suuresta määrästä HLR:ssä ja tietojen purkamisesta jatkokäsiteltävään muotoon. VLR:ssä on vain lista liittymien IMSI-numeroista, mutta tekstiviestin lähetystä varten nämä pitää kääntää vielä MSISDN-numeroiksi HLR:n tai ulkoisten rekisterien avulla. Lyhemmät ajat vaatisivat verkkotoimittajilta tilattavia huoltopäätelaajennuksia keskuksiin. Tiedot voitaisiin myös automaattisesti hakea kerran vuorokaudessa, mutta tällöin ne olisivat pahimmillaan liki vuorokauden vanhoja ja voidaan olettaa, että monen tilaajan liittymän sijainti on jo muuttunut tänä aikana.

LA/SA-tarkkuudella puolestaan alueet pitäisi aina tapauskohtaisesti ensin selvittää radioverkkosuunnittelusta. Kohdealue saattaa jakautua useamman VLR:n alueelle, joten jokaiselta on selvitettävä liittymät samaan tapaan kuin pelkästään VLR:n alueelle suuntautuvassa kyselyssä. Tämän lisäksi jokaisen liittymän sijaintialue (LA/SA) tulee vielä erikseen selvittää MSISDN-numeron avulla tehtävällä kyselyllä HLR:stä. Aikaa kuluu siis kokonaisuudessaan vielä enemmän kuin pelkästään VLR-tarkkuudella tehtävissä hauissa. Vastaavasti solutarkkuudella tehtävässä paikannuksessa tulee ensin suorittaa LA/SA-tarkkuuden menetelmällä kohdealueella olevat liittymät. Sen jälkeen jokainen liittymä tulee paikantaa erikseen verkon toimesta yksitellen liittymää kutsumalla. Paikannusnopeudeksi on arvioitu n. 10 kyselyä sekunnissa (paikannuspalvelu on suunniteltu ensisijaisesti yksittäisten liittymien paikantamiseen, ks. alakohta 3.2.4), joten suurten vastaanottajajoukkojen kohdalla paikantaminen on erittäin hidasta ja siihen liittyvä runsas signalointiliikenne saattaa tukkia

verkkoa muulta liikenteeltä. Menetelmä on käyttökelpoinen lähinnä silloin, kun se voidaan rajoittaa alueille, joissa liittymien määrän tiedetään olevan pieni.

Suorien verkkoelementtikyselyjen lisäksi kohdealueella olevia liittymiä voitaisiin myös selvittää ulkoisen tapahtumienkeruujärjestelmän avulla. Esimerkiksi Nokian verkkoyhtiön tuote NetAct Traffica mahdollistaa päätelaitteiden sijaintitiedon päivitysten keräämisen talteen, jolloin järjestelmästä saadaan suoraan laitteen viimeisin LA/SA tai alueella olevien tilaajien MSISDN-numerot [Viestintävirasto, 2005]. Päätelaitteet raportoivat sijaintitiedon päivityksen (Location Update) yleensä rekisteröityessään verkkoon tai siirtyessään toiselle LA/SA-alueelle, mutta verkon parametreissa voidaan myös määritellä säännöllisesti tapahtuva sijaintitiedon päivitys riippumatta päätelaitteen liikkeistä. Tiedonlähteenä järjestelmä voi käyttää monia erilaisia verkkoelementeiltä saatavia tietoja sekä myös passiivista verkkolinkkien signalointidatan monitorointia. Tällaisten järjestelmien toteutus on kuitenkin operaattorikohtaista ja mikäli sellaisia ei ennestään ole käytössä, ne vaativat huomattavia lisäinvestointeja verkkoon. Samoin järjestelmien integrointi viranomaisten vaaratiedotteiden välitysjärjestelmään vaatisi aina tapauskohtaisen toteutuksen. Ulkoisen tapahtumienkeruujärjestelmän merkittävin etu on kuitenkin huomattavasti verkon omia elementtejä nopeammin (muutamissa minuuteissa) tapahtuva päätelaitteiden MSISDN-numeroiden selvitys LA/SA-tarkkuuteen asti.

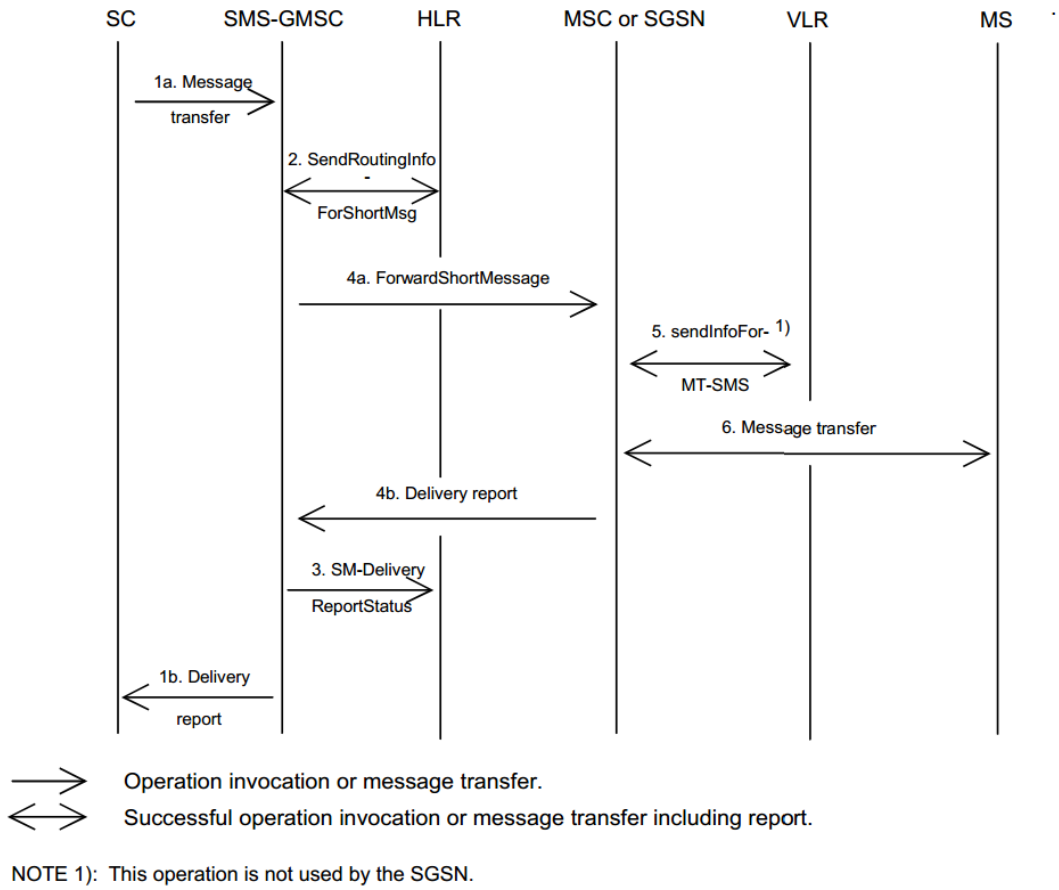
3.3.2. Massatekstiviestien lähetys

Massaviestilähetyksellä tarkoitetaan huomattavalle vastaanottajajoukolle (tuhansia tilaajia) samanaikaisesti lähetettäviä tekstiviestejä. Mikäli alueellisesti kohdennetuissa vaaratiedotteissa päädytään käyttämään normaaleja tekstiviestejä CBS-tekniikan sijaan, viestien suuri määrä muodostaa haasteita niiden nopealle toimittamiselle. Yksittäisen mobiilipäätelaitteeseen toimitettavan tekstiviestin (SMS-MT) välittäminen muodostuu seuraavista vaiheista, jotka on esitetty sekvenssikaaviona kuvassa 8:

1. Tekstiviestikeskus (SC) vastaanottaa välitettävän tekstiviestin. Viestissä on varsinaisen sisällön lisäksi mm. vastaanottajan liittymänumero (MSIDN), lähettäjän numero (vastaanottajalle näkyvä tieto, voi olla myös tekstimuodossa) ja viestin luokka (määrittää muutamia erikoistapauksia kuten flash SMS:n ja silent SMS:n)
2. SC lähettää viestin siihen liitetylle keskukselle (Gateway MSC:lle). SMS-GMSC kysyy kotirekisteri HLR:ltä vastaanottajan numeroon liittyvät reititystiedot (SRI). Tekstiviestin välitys voi tapahtua joko perinteisen MSC-keskuksen kautta tai pakettidatayhteyden avulla SGSN:n välityksellä.

HLR palauttaa ajantasaisen tiedon siitä, mikä MSC ja/tai SGSN tilaajaa palvelee.

3. SMS-GMSC välittää viestin edelleen tilaajaa sillä hetkellä palvelevalle MSC:lle tai SGSN:lle.
4. Palveleva MSC kysyy edelleen paikallisesta vierailijarekisteristä (VLR) tilaajanumeroa (MSISDN) vastaavat tiedot. VLR palauttaa TMSI:n, sijaintialueen ym. reititystiedot paikannettuaan tilaajan päätelaitteen (”paging”). Mikäli tilaajalla on ennestään aktiivinen pakettidatakonteksti käytössä, viesti voidaan reitittää SGSN:n kautta eikä tilaajaa tarvitse erikseen paikantaa. Tällöin viestin välitys on huomattavasti nopeampaa.
5. Palveleva MSC (tai SGSN) välittää viestin päätelaitteelle, joka kuittaa vastaanoton. Keskus välittää edelleen kuittauksen takaisinpäin GMSC:lle, joka puolestaan kuittaa onnistuneen toimituksen SMSC:lle. Mikäli viestin toimitus ei syystä tai toisesta onnistu, SMSC säilyttää viestin ja yrittää lähetystä uudelleen viestiin määritellyn elinajan puitteissa.



Kuva 8. SMS-MT-viestin toimittamisen vaiheet verkossa [ETSI, 2013b]

Tekstiviestin välitys vaatii siis monia samoja toimenpiteitä kuin puhelun vastaanottaminen matkaviestimeen, olennaisimpana verkon toimesta suoritettavan

päätelaitteen kutsuminen (paging) hakemalla ensin laitteen tunnettu sijaintialue VLR:stä ja sen jälkeen kutsumalla päätelaitetta kaikissa LA:n soluissa yleisviestikanavalla. Poikkeuksen muodostavat tilanteet, joissa päätelaitteelta on jo pakettidatayhteys auki ja tekstiviesti voidaan välittää sen kautta. Jokaiselle viestin vastaanottavalle tilaajanumerolle on suoritettava samat toimenpiteet, jotta viesti saadaan perille. Viestinlähetys etenkin samalla kohdealueella oleviin liittymiin ei rinnakkaistu kovin tehokkaasti. Mikäli lähetettäviä viestejä ja vastaanottajia on useita tuhansia, viestien toimittamiseen kuluu runsaasti aikaa, jopa useita tunteja.

Mikäli siis alueellisesti kohdennettuja tekstiviestejä haluttaisiin lähettää tietämättä ennalta alueella olevien tilaajien MSISDN-numeroita, jouduttaisiin tilaajien selvittely tekemään periaatteessa kahteen kertaan, koska verkko ei ilman merkittäviä ohjelmisto- tai palvelumuutoksia muista tilaajien sijaintia siten, että tätä tietoa voitaisiin hyödyntää tekstiviestien toimittamisessa. Päätelaitteen paikantaminen itsessään voidaan kuitenkin tehdä tekstiviestiteknologiaa soveltaen. Ei-aktiivinen päätelaite voidaan pakottaa paikantumaan ja päivittämään sijaintinsa lähettämällä liittymään ns. ”silent SMS”, eli tekstiviesti, joka toimitetaan normaalin viestin tapaan, mutta ei näy päätelaitteessa mitenkään.

3.4. Internet ja viranomaisten verkkopalvelut

3.4.1. Viranomaisten verkkopalvelut Suomessa

Maailmanlaajuinen Internet-tietoverkko on nykyaikaisen informaatioyhteiskunnan selkäranka. Tilastokeskuksen tuoreen tutkimuksen mukaan 92 prosenttia 16–74-vuotiaista suomalaisista käyttää internetiä ja 80 % käyttää sitä päivittäin. Viranomaistietoa oli hakenut 61 prosenttia käyttäjistä. Matkapuhelimella internetiä käytti kodin ja työpaikan ulkopuolella 52 prosenttia edellä mainitusta väestöryhmästä [Tilastokeskus, 2013].

Suomeen Internet ja WWW tulivat alkujaan tiedeyhteisön kautta kansainvälisen esimerkin myötä. Suomen Internet-ajan voidaan katsoa alkaneen syksyllä 1988, kun pohjoismainen yliopistojen ja korkeakoulujen tutkimusverkko NORDUNET ja sen osana Suomen Funet-tietoverkko liitettiin Tukholmasta suoralla satelliittiyhteydellä Yhdysvaltain Internetiin [Ahonen, 2008].

Viranomaisten palveluista verkkoon tulivat ensimmäisinä organisaatioiden lyhyet esittelyt ja yhteystiedot 1990-luvun puolivälissä. Esimerkiksi poliisin verkkosivut osoitteessa *http://www.poliisi.fi* on Web.archive.org-palveluun arkistoidusta kopiosta löytyvän tiedotteen mukaan avattu 8.11.1996. Sisäasiainministeriön verkkosivut on avattu jo tätä aiemmin. Internetistä tuli vuosituhannen

vaihteeseen mennessä myös viranomaisille tärkeä tiedotuskanava, josta löytyivät uusimmat tiedotteet ja julkaisut. Sen sijaan asiointipalveluiden osalta vaihtoehtona oli pitkään lähinnä puhelinnumeroiden listaus, yksittäiset sähköpostiosoitteet tai yleinen palautelomake. Verkkoasiointi pääsääntöisesti erilaisten sähköisten lomakkeiden (ja niihin integroitujen viranomaisten omien tietojärjestelmien) muodossa on yleistynyt vasta 2000-luvulla. Asiointipalveluja vauhdittivat paitsi Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003), myös Valtiovarainministeriön sekä julkisen tietohallinnon neuvottelukunnan (JUHTA) erilaiset hankkeet, joiden tuloksena saatiin vakioidut sähköisen tunnistamisen menetelmät pankkitunnuksin tai sähköisellä henkilökortilla.

3.4.2. Verkkoviestintä ja kriisitilanteet

Julkisen tietohallinnon neuvottelukunnan suositus viranomaisten verkkopalveluista [JUHTA, 2010] linjaa:

> ”Julkisuuslaki ja kuntalaki edellyttävät, että viranomainen tiedottaa aktiivisesti toiminnastaan. Valtion Internetin käyttö- ja tietoturvallisuussuosituksen mukaan viranomaisen tulee tiedottaa myös Internet-verkon välityksellä. Tiedottamisen lisäksi Internet tarjoaa mahdollisuuden kaksisuuntaiseen viestintään, jolloin asiakkaat, kumppanit yms. kohderyhmät pystyvät aikaisempaa paremmin osallistumaan organisaation prosesseihin, toimimaan vuorovaikutuksessa ja asioimaan verkon välityksellä.”

Kansalaisen näkökulmasta viranomaispalvelut ovat pirstoutuneet moneen eri paikkaan, koska verkkopalvelut on rakennettu niitä tuottavien organisaatioiden mukaisesti, ei niinkään sen mukaan, mitä palveluja tarvittaisiin. Useimmat viranomaispalvelut löytyvät oman kotikunnan verkkosivujen kautta (sosiaali- ja terveyspalvelut, pelastustoimi, ympäristönsuojelu), mutta toisaalta jotkin organisaatiot, kuten Hätäkeskuslaitos, Kansaneläkelaitos ja poliisi ylläpitävät itse omia valtakunnallisia verkkosivujaan.

Kuntaliiton [2010] mukaan kriisitilanteessa kansalaiset lähtevät välittömästi etsimään tietoa muualtakin kuin tiedotusvälineiden palveluista. Loogisinta on silloin suunnata sen organisaation, esimerkiksi kunnan, sivuille, jota kriisi koskee tai jonka alueella kriisi on tapahtunut. Poikkeustilanteissa tietoverkkojen etuja ovat nopeus, ja mahdollisuus välittää oma viesti samansisältöisenä laajalle ihmisjoukolle edullisesti. Viranomaisista mm. poliisi on itsekin todennut vuonna 2005, että *”Tiedotus herää tai herätetään myöhään tilanteen osuessa päälle; tiedotuksen tehtävät ja resurssit poikkeustilanteissa ovat epäselvät”* sekä *”Internet-valmiudet eivät ole riittäviä tehostettua viestintää vaativissa olosuhteissa”* [Poliisi, 2009]. Tilanne on toki parantunut tämän jälkeen jossakin määrin, mutta

edelleen yllättävissä ja nopeaa toimintaa edellyttävissä kriisitilanteissa tiedotuksessa on haasteita.

Viranomaisten verkkosivujen ohjeistuksissa esitetään usein malli erillisestä ns. kriisisivustosta tai -portaalista, joka voidaan ottaa käyttöön poikkeustilanteissa. Tällaisen etuna on Kuntaliiton [2010] mukaan nopea käyttöönotto, kun portaalin rakenne on jo valmiina ja sinne tarvitsee vain lisätä tapahtumakohtaiset tiedot. Portaali on rakenteeltaan kevyt, jotta se latautuisi nopeasti. Toisaalta kaikki poikkeustilat eivät edellytä kriisiportaalin käyttöä, vaan tietoa voidaan jakaa myös pysyvän turvasivuston tai erilaisten teemasivustojen välityksellä.

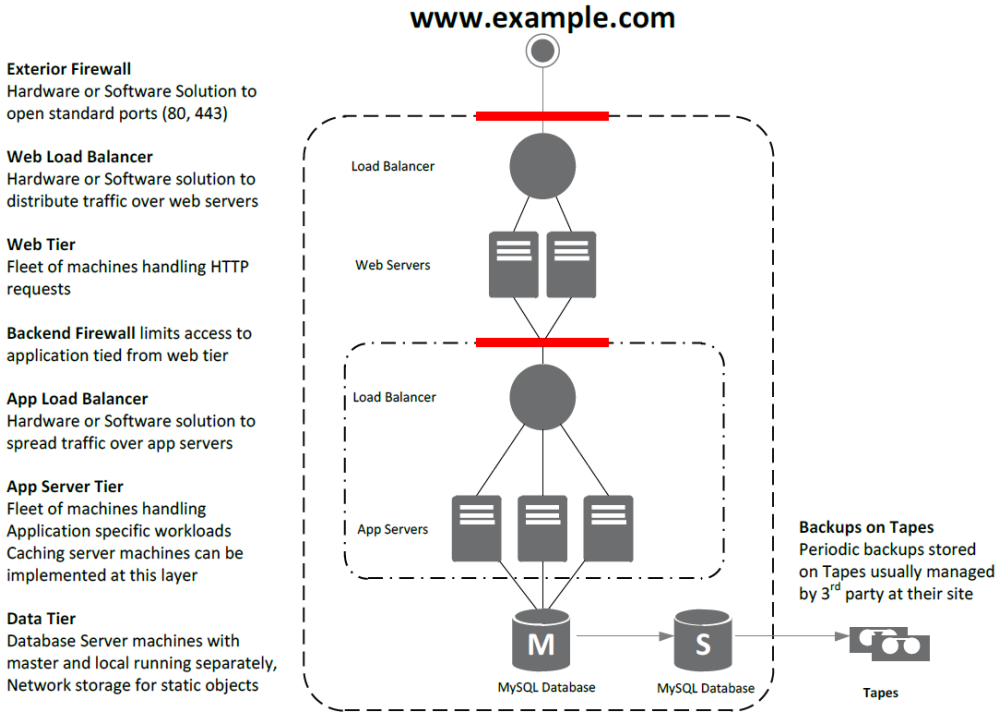
3.4.3. Verkkopalvelun tekninen toteuttaminen

Yksinkertaisimmillaan verkkopalvelu on jatkuvasti Internetiin liitetty tietokone, joka ajaa web-sisällön tarjoiluun HTTP-protokollalla soveltuvaa palvelinohjelmistoa. Palvelun löytämiseksi organisaatio yleensä rekisteröi nimiinsä helposti muistettavan verkko-osoitteen (esimerkiksi *poliisi.fi*), määrittää www-palvelimilleen verkko-osoitetta vastaavat IP-osoitteet ja päivittää nämä DNS-nimipalveluunsa. Tämän jälkeen on vielä reitityksen ja palomuurien osalta huolehdittava siitä, että www-palvelin on tavoitettavissa kaikkialta internetistä ainakin HTTP- ja usein myös salatulla HTTPS-protokollalla. Tietoturvasyistä pääsy julkisesta verkosta organisaation omaan verkkoon pidetään yleensä hyvin minimaalisena ja vain välttämättömät palvelut avataan. Tavallista on, että www-palvelinten kaltaiset julkiset palvelut sijoitetaan erilleen ns. DMZ-verkkoon (de-militarized zone), tai kokonaan organisaation ulkopuolisen erillisen palveluntarjoajan vastuulle.

Yksinkertaisia staattisia resursseja (HTML-sivuja, kuvatiedostoja ym.) tarjoileva palvelu kestää helposti nykyaikaisilla palvelintietokoneilla tuhansia sivupyyntöjä sekunnissa. Verkkopalvelujen taustalle on kuitenkin yleensä sisällön ylläpidon helpottamiseksi tai sähköisen asioinnin mahdollistamiseksi toteutettu monimutkaisempi tietojärjestelmä, joka rakentaa käyttäjälle lähetettävän HTML-dokumentin dynaamisesti jokaisella hakukerralla hakien sisältöä taustalla esimerkiksi tietokannoista ja muista tietojärjestelmistä. Toteutuksesta riippuen yksittäinen sivupyyntö voi viedä moninkertaisesti enemmän laiteresursseja kuin staattisten sivujen tarjoilu, ja tällaisen dynaamisen verkkopalvelun yhtäaikaisten käyttäjien kestokyky jääkin paljon staattista alhaisemmaksi. Suorituskyvyn tehostamiseksi sekä hallinto- tai tietoturvasyistä palvelu on hajautettava useammalle fyysiselle palvelimelle.

Kuvassa 9 on esitetty yleistetty esimerkki perinteisestä kolmikerroksisesta verkkopalveluarkkitehtuurista keskisuurelle verkkopalvelulle, jossa arkkiteh-

tuuri on hajautettu vertikaalisesti esitys-, sovellus- ja tietovarastokerroksiin. Horisontaalinen skaalautuvuus on myös huomioitu kuormanjakajilla ja usealla rinnakkaisella palvelimella eri kerroksissa [Tavis & Fitzsimons, 2012].



Kuva 9. Perinteinen verkkopalvelun arkkitehtuuri [Tavis & Fitzsimons, 2012]

Nykyään verkkopalveluita toteutetaan usein myös virtualisoimalla palvelimia, jolloin yhdellä fyysisellä palvelinalustalla voidaan ajaa useita toisistaan loogisesti erillisiä palvelimia. Ratkaisun etuna on laiteresurssien konsolidointi ja jakaminen usean palvelun kesken sekä ketterä siirrettävyys alustalta toiselle. Virtualisointiteknologioiden päälle rakentuvat esimerkiksi Amazonin kaltaiset pilvipalvelut, joille on ominaista ketterä skaalautuvuus sekä käyttöpohjainen laskutus [Kurtti, 2013].

3.4.4. Korkean saatavuuden verkkopalvelut

Verkkopalvelun saatavuutta kaikissa tilanteissa, myös yllättävissä kuormituspiikeissä joko palvelunestohyökkäyksen tai suurta yleisöä äkillisesti kiinnostavan sisällön kohdalla, voidaan parantaa lukuisin keinoin. Jotkin pullonkaulat ovat valitettavasti sidoksissa käytettyihin laitekomponentteihin, julkaisujärjestelmäohjelmistoihin tai muihin taustajärjestelmiin, mutta seuraavassa esitän joitakin yleisempiä ongelmia ja ratkaisuja niihin.

Varsinainen Internet-yhteys harvoin muodostuu siirtonopeuden osalta enää nykyään pullonkaulaksi, mutta sen sijaan aktiivilaitteet, ennen kaikkea palomuurit ja reitittimet, saattavat ylläpitää ns. tilataulua aktiivisista yhteyksistä. Mikäli uusien yhteyksien määrä kasvaa yllättäen joko palvelunestohyök-

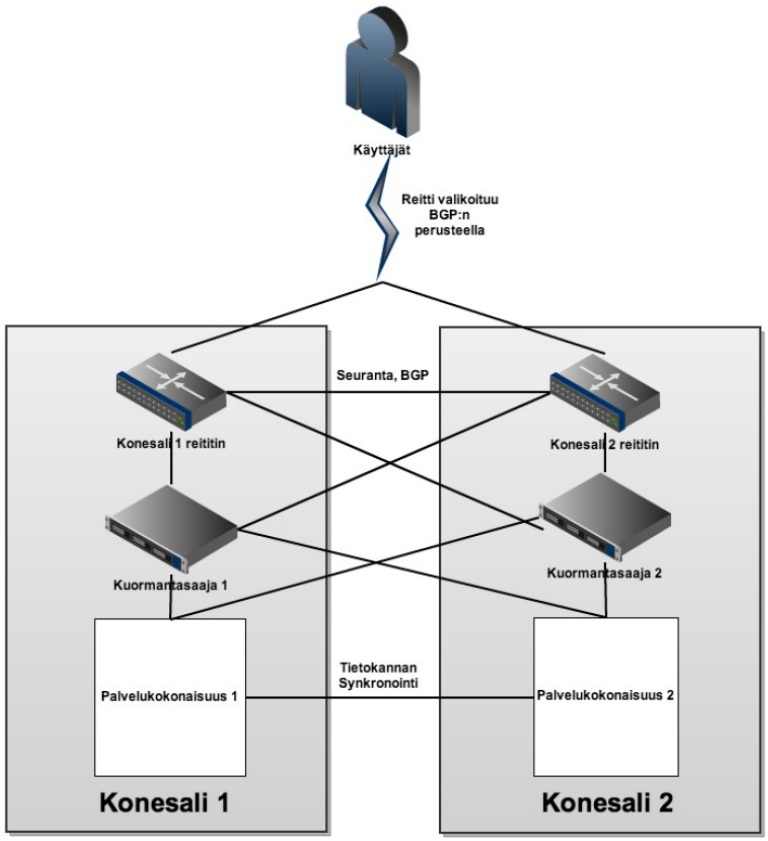
käyksestä tai oikeiden käyttäjien kiinnostuspiikistä johtuen, väärin mitoitettu palomuuri saattaa asettaa ylärajan verkkopalvelun yhtäaikaisille käyttäjille jo paljon ennen varsinaisia verkkopalvelimia. Tilallisten palomuurien sijaan yksinkertaiset, tilattomiin pääsylistoihin perustuvat rajoitukset verkosta maailmalle tarjottavien palvelujen edessä ovat skaalautuvampi ratkaisu. Samaan tapaan itse verkkopalvelussa tulee välttää tilatietoisia toteutuksia, sillä niiden hajauttaminen usealle palvelimelle muodostuu monimutkaiseksi ja riskialttiiksi.

Internet-yhteys voidaan myös kahdentaa usean operaattorin kautta (mikä on mielekästä ennen kaikkea mahdollisten vikatilanteiden varalta) BGP-tekniikalla, ja tarvittaessa tarjoilla yhtäaikaisesti eri yhteyksien kautta sisältöä eri operaattoreilta tuleville kävijöille. Suuret globaalille asiakaskunnalle suunnatut verkkopalvelut voivat hyödyntää Akamai Technologiesin tai Amazon CloudFrontin kaltaisia palveluita, joissa verkkopalvelun sisältö (tai osa siitä, esim. isokokoiset mediatiedostot) peilataan lukuisille hajautetuille CDN-palvelimille (Content Delivery Network) ympäri maailmaa, jolloin asiakkaat saavat sisältönsä aina verkkotopologisesti lähimmältä palvelimelta.

Suuria kävijämääriä kestävän palvelinympäristön tulee skaalautua sekä horisontaalisesti että vertikaalisesti. Vertikaalisessa mielessä eri palvelukerrosten välille voidaan lisätä nopeita välimuisteja (cache), jolloin yhden alemman kerroksen hakupyynnön vastaus voidaan palauttaa suoraan välimuistista lukuisille samoilla parametreilla tehdyille kyselyille ilman, että taustajärjestelmän pitää prosessoida jokaista identtistä pyyntöä erikseen. Hajauttamalla verkkopalvelun sisällön rakentaminen useaan eri tasoon (front-end, back-end, tietokannat) ja sijoittamalla jokaisen eteen välimuistipalvelu saadaan suorituskykyä usein kasvatettua helposti useita kertaluokkia suuremmaksi. Luonnollisesti verkkopalvelun sovelluslogiikka tulee kuitenkin suunnitella sellaiseksi, että se voidaan hajauttaa monelle tasolle. Vastaavasti jokaisella tasolla tulisi voida monistaa toimintalogiikkaa useaan rinnakkaiseen noodiin, jolloin saadaan horisontaalista skaalautuvuutta. Ongelmaksi muodostuvatkin usein vanhat julkaisujärjestelmät, jotka monoliittisina sovelluksina eivät anna mahdollisuuksia vertikaaliseen skaalaukseen ja horisontaalinenkin saattaa vaatia mittavia lisäinvestointeja.

Valtionhallinnon VAHTI-tietoturva- ja varautumisohjeet määrittelevät valtion ICT-järjestelmille viisiportaisen varautumistaulukon. Sen keskimmäisellä tasolla (”korotettu”) ovat esimerkiksi kansalaisille poikkeustilanteissa keskeiset palvelut. Niitä tulee seurata ympärivuorokautisesti, eivätkä ne saa olla riippuvaisia tietoliikenneyhteyksistä Suomesta ulkomaille [Kurtti, 2013]. Viimeisin ehto sulkee pois globaalien toimijoiden, kuten Amazonin, pilvipalvelut ainoana toteutustapana, mutta näitä voidaan kuitenkin hyödyntää normaalitilanteissa

palvelun nopeaan horisontaaliseen skaalaukseen. Korkean saatavuuden järjestelmien toteutuksessa otetaan huomioon myös infrastruktuuriin (sähkönsyöttö, laitetilat, tietoliikenneyhteydet, tallennus- ja palvelinlaitteet) liittyvät riskit kahdentamalla eri konesaleihin kaikki järjestelmän toiminnan kannalta kriittiset komponentit (ks. kuva 10). Kahdennuksessa on huomioitava täydellinen hajautus siten, että mikään kahdennettu osa ei ole riippuvainen samoista resursseista (erilliset sähkönsyöttöjärjestelmät ja kaapelireitit).



Kuva 10. Korkean saatavuuden infrastruktuurin arkkitehtuuri [Kurtti, 2013]

Perinteisesti täysin kahdennetun palvelinympäristön ratkaisut ovat muodostuneet melko kalliiksi, mutta virtualisoimalla palvelinalustat voidaan saavuttaa merkittäviä kustannushyötyjä useiden palvelujen jakaessa samat vakioidut fyysiset resurssit. Tällöin tulee kuitenkin kiinnittää erityistä huomiota palveluiden tietoturvaan sekä laiteresurssien riittävyyteen. Toisaalta virtualisoitu palvelinpaketti tukee myös ketterästi nopeaa skaalautuvuutta mahdollistaen esimerkiksi koko toteutuksen siirtämisen toisen palveluntarjoajan konesaliin tai pilvipalveluun.

4. Väestöhälytys- ja vaaratiedotejärjestelmä

"There goes the siren that warns of the air raid. Then comes the sound of guns sending flak."

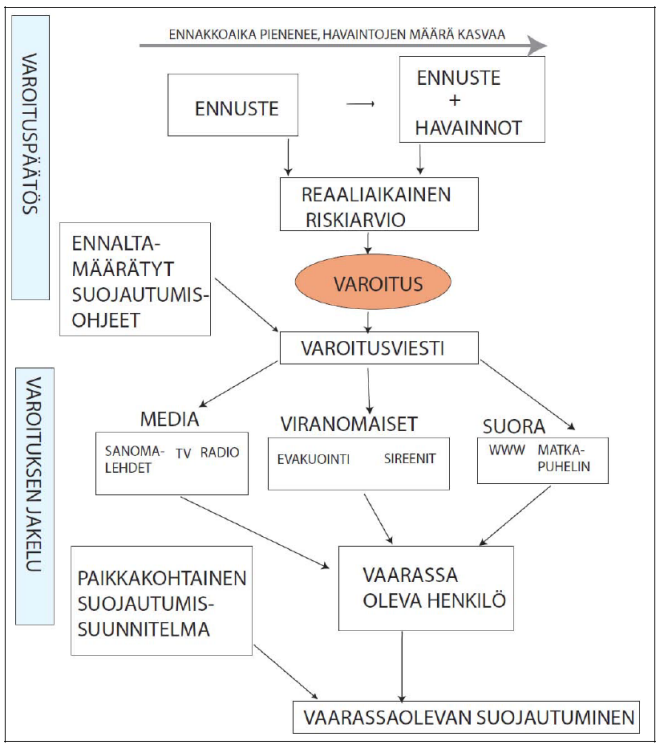
Iron Maiden – Aces High

Väestöhälytysjärjestelmien historia ulottuu satojen vuosien taakse. Varhaisena esimerkkinä voidaan pitää kirkonkellojen tai erillisten varoituskellojen soittoa kellotornissa, ja joissakin maissa tällaiset varoitustavat ovat edelleen käytössä. Kellojen soitto välitti kuitenkin ainoastaan tiedon siitä, että jotakin tärkeää oli tapahtumassa, muttei tarkempaa tietoa tapahtuman laadusta. Saadakseen tietoja tapahtumasta ja toimintaohjeita asukkaiden piti kokoontua esimerkiksi toriaukioille, jossa tarkempi tieto levisi suullisesti. Esimerkki kuvaa väestöhälytysjärjestelmien kahta eri ulottuvuutta: kellojensoitolla voidaan varoittaa maantieteellisesti melko suurta aluetta, mutta niiden avulla voidaan välittää hyvin rajallinen määrä informaatiota. Yksityiskohtainen tieto ja toimintaohjeet puolestaan välitettiin suullisesti, mutta tämä tavoitti vain pienelle alueelle kokoontuneen rajallisen väkijoukon [CHORIST, 2008].

Edellisessä luvussa esitin viestintäteknologian teknistä taustaa niin matkaviestinverkoissa kuin Internetissäkin. Kohdennetuissa vaaratiedotteissa pyritään perinteisten joukkotiedotusvälineitä tai julkisia hälyttimiä käyttävän viestinnän sijaan saamaan viesti suoraan valitulla alueella oleville ihmisille. Matkaviestinten reaaliaikainen paikantaminen on nykyisissä GSM/UMTS-verkoissa haastavaa ja viestien välittäminen kymmeniin tuhansiin liittymiin voi myös kestää. Tätä viivettä pyritään kuitenkin eliminoimaan välittämällä viesti samanaikaisesti muiden eri kanavien (televisio, radio, www-sivut, sosiaalinen media) kautta, jolloin eri viestintämuodot tukevat toisiaan. Kun hätäviestinnän toteuttamisessa huomioidaan alusta alkaen eri kanavat, todennäköisyys viestin perille menolle kasvaa huomattavasti. Tässä luvussa esittelen vaaratiedotejärjestelmään liittyviä hankkeita maailmalta sekä hahmottelen järjestelmän ominaisuuksia ja vaatimuksia. Seuraavassa luvussa puolestaan luonnostelen Suomen oloihin sopivan järjestelmän arkkitehtuuria.

Perinteiset väestöhälytysjärjestelmät ovat olleet sireenipohjaisia ulkohälyttimiä, joilla on voitu välittää vaaramerkki tilanteissa, jotka edellyttävät välitöntä suojautumista. Sireenit otettiin käyttöön alkujaan toisen maailmansodan aikana varoittamaan ilmapommituksista ja järjestelmiä kehitettiin ja laajennettiin runsaasti kylmän sodan aikana. Sireenihälytyksiä on käytetty myös rajatummilla alueilla, esimerkiksi teollisuuslaitoksissa, varoittamaan paikallisista vaaratilanteista. Joukkoviestimien kehittymisen myötä hätätiedotteita on alettu välittää myös radiossa ja televisiossa. Suomeen televisiolähetysten ohessa välitettä-

vät hätätiedotteet saatiin verrattain myöhään, vasta vuonna 2009, ja tämäkin järjestelmä toimii vain valtakunnallisella tarkkuudella. Matkapuhelinverkon käytöstä hätätiedottamiseen on myös ollut erinäisiä hankkeita, mutta vielä toistaiseksi tästä ei ole yleisiä käytäntöjä. Johdantoluvussa on kuvattu Suomessa käynnissä olleita tekstiviestivaroitushankkeita ja niihin liittyviä ongelmia. Matkaviestimien lisäksi keskustelua on käyty myös internetin hyödyntämisestä hätätiedottamisessa. Yksi ongelmista on tiedottamisen jakautuminen usealle eri viranomaiselle (kunnat, pelastuslaitokset, poliisi, ministeriöt).



Kuva 11. Vaarallisten luonnonilmiöiden varoitusprosessi [Huovila ja muut, 2010]

Vaaratiedote ja sen välitys vaarassa oleville on vain osa varoitusprosessia, joka alkaa vaaratilanteen syntymisestä ja sen havaitsemisesta, ja päättyy vaarassa olevien suojautumiseen tai muihin tilanteen vaatimiin toimenpiteisiin varoituksen seurauksena. Kuten seuraavissa alakohdissa käy ilmi, monissa ulkomaisissa varoitusjärjestelmähankkeissa on keskeisenä osana myös vaaratapahtumien (lähinnä luonnononnettomuuksien) automaattinen havainnointi ja riskiarviointi ennen varsinaista varoituksen antamista. Suomen oloissa onneksi ainakin toistaiseksi äärimmäiset luonnonilmiöt ovat sen verran harvinaisia ja suhteellisen hitaasti kehittyviä, että niistä varoittamiseen riittävät Ilmatieteen laitoksen antamat vaaratiedotteet. Huovila ja muut [2010] ovat pilotoineet UHHA-hankkeessa Suomen oloihin tarkoitettua uhkatilanteen hallinta-, hälytys-, tilannekuva- ja varoitusjärjestelmän kehittämistä luonnon- ja teollisuusonnetto-

muuksien automaattisen havainnointiin ja varoittamiseen. Heidän esittämänsä varoitusprosessin kuvaus (kuva 11) on hyvin sovellettavissa myös muihin vaaratiedotteisiin, esimerkiksi uhkaavasta henkilöstä varoittamiseen. Mallissa on jo huomioitu perinteisten median ja viranomaistiedotuksen lisäksi myös suora tiedottaminen matkapuhelimilla tai WWW:n (Internetin) välityksellä.

4.1. Japanin ETWS

Pisimmällä väestöhälytysjärjestelmissä ainakin luonnononnettomuuksista varoittamisen kannalta on Japani. Niin pitkälle kuin historiankirjoitusta riittää, löytyy mainintoja tuhoisista onnettomuuksista kuten tulivuorenpurkauksista, maanjäristyksistä ja tsunameista johtuen Japanin sijainnista mannerlaattojen liikkumakohdan reunalla. Tästä johtuen japanilaisilla on aivan eri tavalla kulttuurisesti sisäänrakennettuna suhtautuminen luonnononnettomuuksiin ja niihin varautuminen. Jokainen uusi katastrofi toimii kovana opetuksena parantaa rakennusten turvallisuutta ja varautumistekniikoita.

Nykyinen vuodesta 2007 toiminut ETWS-järjestelmä (Earthquake and Tsunami Warning System, joissakin yhteyksissä myös Earthquake Early Warning System EEWS) on Japanin meteorologisen laitoksen (JMA) ja teleoperaattori NTT DOCOMOn ylläpitämä, ja se koostuu koko maan kattavasta seismisten sensorien verkosta. Niiden keräämä raakadata välitetään analyysijärjestelmään, joka tulkitsee mahdollisen maanjäristyksen sijainnin ja voimakkuuden sekä ennustetun vaikutusalueen. Seismiset värähtelyt kulkevat maankuoressa n. 2-5 km/s nopeudella, joten automatisoidulla sähköisellä varoitusjärjestelmällä on mahdollista ehtiä antamaan täpärästi varoitus juuri ennen, kuin järistys osuu alueelle. Ennakkovaroituksen saatuaan esimerkiksi junat ja pilvenpiirtäjien hissit pysähtyvät automaattisesti ja sairaaloissa ja kouluissa voidaan varautua ripeästi.

Automaattiset varoitukset lähtevät kaksiportaisesti. Jos ensimmäinen ennuste antaa olettaa vähintään 3,5 magnitudin järistystä, lähtee ennakkovaroitus tietoverkkoyhteydellä pienemmälle vastaanottajajoukolle, joka on ennalta tilannut varoitukset. Tähän kuuluvat mm. automaattijärjestelmät junien pysäyttämiseksi, tutkimuslaitokset, pelastusviranomaiset, sairaalat yms. tahot. Uusien havaintojen myötä lähetetään päivitettyjä varoituksia, ja vastaanottajien tietokoneet voivat myös paikallisesti arvioida vaikutusta sijainnin perusteella. Laajamittaisempi varsinainen maanjäristysvaroitus annetaan, jos magnitudin 5 järistys on havaittu vähintään kahdella eri havaintoasemalla (virheellisten hälytysten välttämiseksi). Tämä väestöhälytys välitetään useiden eri kanavien kautta, mm. perinteisten kovaäänisten väestöhälyttimien avulla, televisiossa sekä radiossa. Japanin ikääntyvän väestön vuoksi perinteiset viestintäväylät ovat

tärkeitä. Lisäksi varoitus välitetään matkapuhelinverkossa cell broadcast -tekniikalla, jota useimmat operaattorit tukevat. Käyttäjien tulee kuitenkin useimmissa päätelaitteissa itse aktivoida toiminnot viestien vastaanottamiseksi.

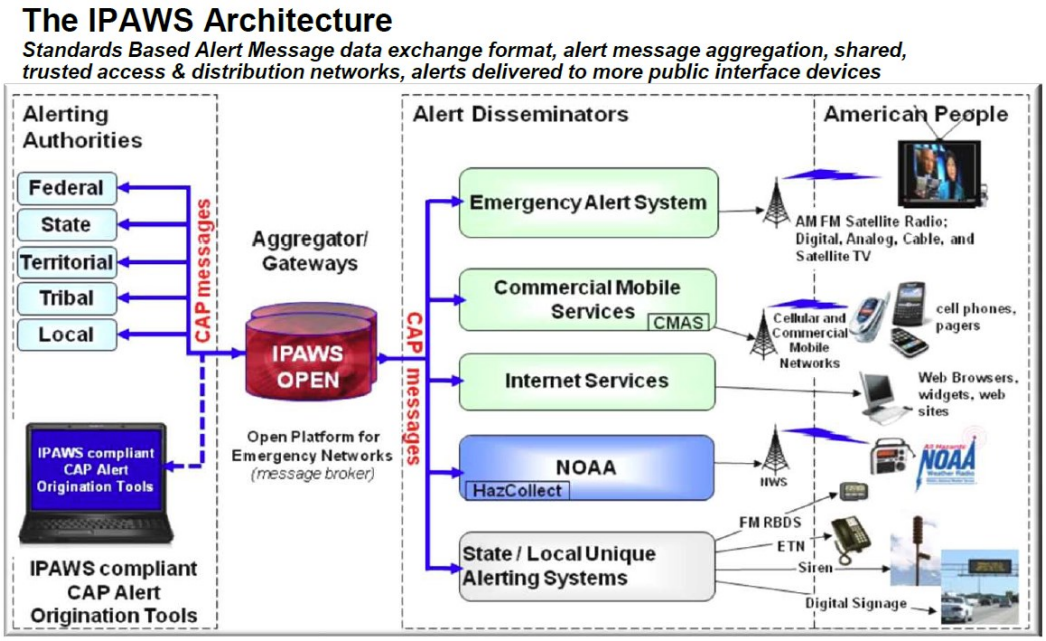
Keväällä 2011 Tohukun maanjäristyksen yhteydessä varoituksen sai matkapuhelimen kautta arviolta 52 miljoonaa ihmistä. Huolimatta nopeasta ja tehokkaasta varoitusjärjestelmästä, puutteita löytyi sensoridataa analysoivasta järjestelmästä, joka ei tuolloin osannut ennustaa tarpeeksi vakavana laajamittaisen siirroksen aiheuttamaa järistystä ja hyökyaaltoa [Yamazaki, 2012].

4.2. Yhdysvaltain IPAWS ja CMAS/WEA-hankkeet

Presidentti George W. Bushin määräyksestä Yhdysvaltain Department of Homeland Security käynnisti vuonna 2006 laajamittaisen IPAWS-hankkeen. (*Integrated Public Alert and Warning System)*. Sen liikkeellepanijana oli aiempana vuonna laajoja tuhoja aiheuttaneen hirmumyrsky Katrinan jälkiselvittelyssä esiin noussut kritiikki viranomaistoiminnasta. Yhdysvaltain järjestelmien kehityksen taustalla vaikuttavat myös terrorismin uhat; modernisoitua hätätiedotusjärjestelmää on sikäläisessä julkisessa keskustelussa kaivattu erityisesti vuoden 2001 syyskuun 11. päivän iskuista lähtien. Hankkeen tavoite on tiivistetysti:

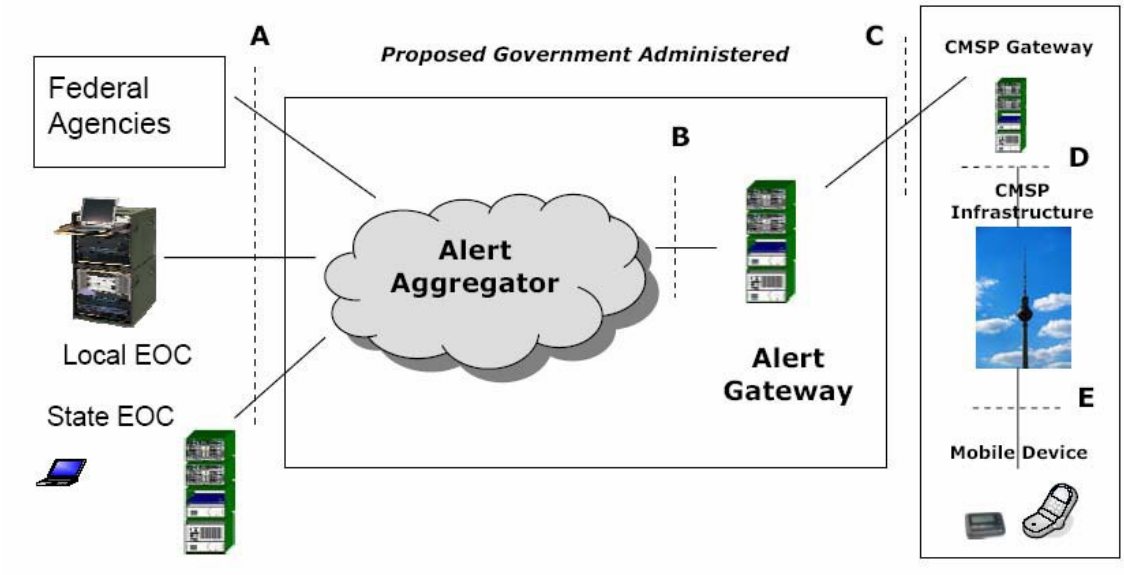
> "Provide integrated services and capabilities to local, state, and federal authorities that enable them to alert and warn their respective communities via multiple communications methods." [FEMA, 2011]

IPAWS hyödyntää puolestaan Yhdistyneiden kansakuntien alaisuudessa toimivan ITU:n (*International Telecommunication Union*) standardoimaa CAP-viestiformaattia (*Common Alert Protocol*), joka määrittää yksinkertaisen vakiomuotoisen rakenteisen hätäviestidokumentin. IPAWS-hankkeessa kehitettävän järjestelmän yleisarkkitehtuurin (ks. Kuva 12) keskeisenä osana on avoin CAP-protokollaa käyttävä viestinvälitysalusta OPEN (*Open Platform for Emergency Networks)*, joka kokoaa yhteen eri viranomaisten tuottamat hälytykset ja välittää ne puolestaan edelleen eteenpäin erilaisiin levityskanaviin.



Kuva 12. IPAWS-järjestelmän arkkitehtuuri [FEMA, 2011].

IPAWS-hankkeen ohessa konkreettisia sijaintipalveluita hyödyntäviä viranomaishankkeita ovat E911 ja CMAS. Perinteistä Yhdysvaltain hätänumerototeutusta laajentanut E911 (Enhanced 911) muistuttaa eurooppalaista hätäpaikannusta, ja se onkin osaltaan vaikuttanut täkäläiseen kehitykseen ja 3GPP:n standardointiin. Matkaviestinverkoissa E911:n vaatimus soittajan automaattisesta paikantamisesta on toteutettu kahdessa vaiheessa. Ensimmäisessä vaiheessa operaattorien tuli tarjota hätäkeskukselle tieto soittajan numerosta (ns. call-back number, joka ei välttämättä ole sama kuin tilaajan MSISDN) sekä soittajan käyttämän tukiaseman tai solun sijaintitieto kuuden minuutin kuluessa. Toisessa vaiheessa soittajan sijainti paikannetaan 300 metrin tarkkuudella joko verkko- tai hybridipaikannuksen avulla. E911:n toisen vaiheen käyttöönoton määräaika teleoperaattoreille oli syyskuussa 2012, neljä vuotta alkuperäisestä aikataulusta jäljessä. Näiden jälkeen on aloitettu Next Generation 911 (NG911) projekti, jossa keskitytään IP-hätäpuhelujen ohjaamiseen ja soittajan paikantamiseen [FCC, 2013]. Paikkatietoa käytetään myös ohjaamaan hätäpuhelu soittajaa lähellä olevalle hätäpuhelujen vastaanottajalle [Wong, 2013], sillä Yhdysvalloissa ei ole toistaiseksi käytössä Suomen kaltaisia kaikkien viranomaisten yhteisiä, suuren toiminta-alueen hätäkeskuksia. Esimerkiksi Kaliforniassa on Wongin mukaan 455 erillistä viranomaisten hätäkeskusta, joihin hätänumero 911 voi ohjautua.



Kuva 13. CMAS:n referenssiarkkitehtuuri 3GPP:n [2011] mukaan.

Yhdysvallat on myös ollut edelläkävijä CBS-mobiilihälytystekniikan käyttöönotossa. IPAWS-projektin osana syntynyt CMAS (Commercial Mobile Alert System, sittemmin nimetty uudelleen Wireless Emergency Alerts, WEA) mahdollistaa vaaratiedotteiden välittämisen matkaviestimiin liittovaltion viranomaisten ylläpitämän järjestelmän kautta. Sen referenssiarkkitehtuuri on otettu mukaan myös 3GPP:n [2011] tekniseen dokumentaatioon (kuva 13). WEA-tekniikkaa tukevat päätelaitteet ilmaisevat saapuneen vaaratiedotteen normaalista tekstiviestistä poikkeavalla hälytysäänellä ja näytöllä näkyvällä viestillä (kuva 14). WEA-hälytykset on jaettu kolmeen kategoriaan:

1. Yhdysvaltain presidentin antamat kansallista turvallisuutta koskevat hälytykset. Tulee näyttää lakisääteisesti Yhdysvalloissa kaikissa WEA-tuellisissa päätelaitteissa riippumatta käyttäjän asetuksista.
2. Välitöntä hengenvaaraa koskevat hälytykset. Käyttäjä voi valita, näytetäänkö hälytyksiä.
3. AMBER-hälytykset (ilmoitukset siepatuista lapsista). Käyttäjä voi valita, näytetäänkö hälytyksiä.

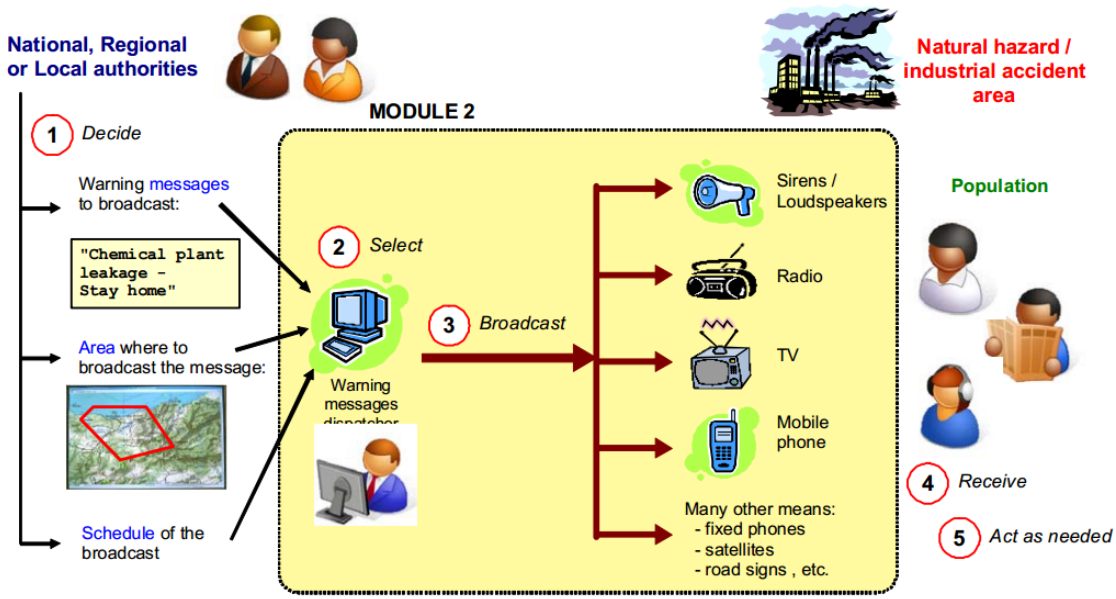
Kuva 14. Esimerkki WEA-hälytyksesta puhelimen näytöllä [FEMA, 2013]

IPAWSin alaisuuteen kuuluvat myös vakioidut rajapinnat IPAWS-OPEN -osaprojektin (Open Platform for Emergency Networks) puitteissa. Yhteinen vakioitu CAP-viestiformaatti tarkoittaa, että kaupallisten laite- ja ohjelmistotoimittajien on helppo tarjota erilaisia tuotteita viranomaistarpeisiin ja järjestelmät ovat keskenään yhteensopivia. Olemassa olevat varoitusjärjestelmät (esim. hälytyssireenit ja tienvarsinäytöt) voidaan myös päivittää IPAWS-OPEN yhteensopiviksi. Käytännön esimerkkinä IPAWS:in avoimista rajapinnoista hälytysten levittämiseen hakukone Google lisäsi karttapalveluunsa Yhdysvaltain viranomaisten tuottamat tulva-, sää- ja maanjäristysvaroitukset tammikuussa 2012 [Google, 2012].

4.3. Euroopan Unionin hankkeet ja EU-ALERT

Euroopan alueella on myös ollut lukuisia osin päällekkäisiä projekteja varoitus- ja hälytysjärjestelmien tutkimiseksi ja standardoimiseksi. Esimerkiksi Euroopan komission rahoittamassa CHORIST-projektissa (Integrating Communications for Enhanced Environmental Risk Management and Citizens Safety, 2006–2009) selvitettiin ympäristö- ja teollisuusriskien hallintaa ja esitettiin ratkaisumalleja onnettomuustilanteiden hallinnan tehokkuuden ja nopeuden parantamiseksi. Projektin 16 jäsentä koostuivat eurooppalaisista viestintäjärjestelmäalan yrityksestä sekä tutkimusorganisaatioista. Suomesta mukana olivat Teknillisen korkeakoulun (nyk. Aalto-yliopisto) tietoliikennelaboratorio ja Nokian TETRA-järjestelmät hankkinut EADS Secure Networks Oy. CHORIST-projekti jakautui kolmeen päämoduuliin: 1. Riskien arviointijärjestelmät, 2. Väestön varoitusjär-

jestelmät ja 3. Nopeasti käyttöönotettavat kenttäviestintäjärjestelmät. Olennainen tämän tutkielman kannalta oli moduuli 2, jonka liittyminen CHORIST-hankkeen kokonaisuuteen on esitetty kuvassa 15. Kuten muutkin vastaavat tutkimukset, tässäkin suositetaan viestin välittämistä mahdollisimman monen eri kanavan kautta perillemenon varmistamiseksi.



Kuva 15. CHORIST-varoitusjärjestelmä [CHORIST, 2008]

Standardointiorganisaatio ETSIn alainen EMTEL-komitea puolestaan on kehittänyt eurooppalaisia standardeja hätäviestintään vuodesta 2005 lähtien. ETSI päätyi EU-ALERTin toteutuksessa Japanin EEWS:n ja Yhdysvaltain CMASin pohjalta myös CBS-teknologian käyttöön perinteisten SMS-viestien sijaan. Pilottiprojektina toimii Hollannin NL-Alert -järjestelmä, joka rakentuu olemassa olevien muiden järjestelmien rinnalle. ETSIn mukaan Hollannin hallitus ”uskoo vahvasti monikanavaiseen lähestymistapaan optimoidakseen väestön tavoitettavuuden” [ETSI, 2012]. EU-ALERTista pyritään kehittämään yhteensopiva Yhdysvaltain WEA:n kanssa ja tulevissa versioissa tutkitaan uusina ominaisuuksina mm. multimediasisällön tuomista mukaan varoitusviesteihin.

5. Vaaratiedotejärjestelmä Suomen tarpeisiin

"Mikäli kohtaat karhun, käyttäydy rauhallisesti ja istu pöytään."

Mainosteksti olutravintolan lasinalusessa

Aiemmissa luvuissa esitettyjen teknologioiden ja kansainvälisten sekä kansallisten hankkeiden pohjalta olen lähtenyt kartoittamaan vaatimuksia Suomen oloihin ja viranomaistarpeisiin soveltuvalle vaaratiedotteiden välitysjärjestelmälle. Näiden vaatimusten perusteella olen määritellyt edelleen järjestelmän arkkitehtuuria korkealla tasolla.

5.1. Tietojärjestelmien vaatimusmäärittely

Yleisesti minkä tahansa tietojärjestelmän suunnittelun lähtökohdaksi tulee määritellä järjestelmän keskeiset toiminnalliset vaatimukset, ympäristövaatimukset sekä laatuvaatimukset ja rajoitteet. Näiden pohjalla ovat järjestelmän käyttötarpeet, joita olen kuvannut aiemmissa luvuissa. Näihin on vielä syytä lisätä järjestelmän helppokäyttöisyys myös sitä operoivien viranomaisten kannalta. Tietojärjestelmän suunnittelussa on huomioitava järjestelmäkokonaisuus, ei pelkästään ohjelmistoa. Yhtenä esimerkkinä tästä voidaan käyttää Pressmanin [2000] jaottelua tietojärjestelmän neljästä peruselementistä:

- *Ohjelmisto*. Tietokoneohjelmat, tietorakenteet ja niihin liittyvä dokumentaatio.
- *Laitteisto*. Tietokoneet, jotka suorittavat ohjelmistoa, niitä yhdistävät tietoverkkolaitteet, sekä järjestelmän reaalimaailmaan yhdistävät laitteet kuten sensorit tai tietokoneen ohjaamat moottorit.
- *Ihmiset.* Järjestelmän loppukäyttäjät ja operoijat.
- *Tietokanta.* Organisoitu kokoelma dataa, jota käsitellään ohjelmiston välityksellä.

Näiden käyttöä puolestaan kuvaavat Pressmanin jaottelussa:

- *Dokumentaatio.* Kuvaava informaatio järjestelmän käytöstä ja operoinnista.
- *Menetelmät.* Vaiheet, jotka määrittävät järjestelmän elementtien tietyn käytön tai järjestelmän menetelmällisen kontekstin.

Tietojärjestelmien vaatimukset jaotellaan usein myös toiminnallisiin ja ei-toiminnallisiin vaatimuksiin. Näistä ensimmäiset kuvaavat varsinaisen järjestelmän toiminnan kattavasti ja yksityiskohtaisesti esim. käyttötapausten avulla. Ei-toiminnalliset vaatimukset ovat puolestaan laatuvaatimuksia koko järjestelmälle ja sen arkkitehtuurille. Ne voivat liittyä esimerkiksi skaalautuvuuteen, tietoturvaan, ylläpidettävyyden tai suorituskykyyn. Ei-toiminnalliset vaati-

mukset asettavat rajoitteita ja reunaehtoja varsinaisen tietojärjestelmän tekniselle toteutukselle.

5.2. Vaaratiedotejärjestelmän vaatimukset

Suomen tarpeisiin sovellettu vaaratiedotejärjestelmä rakentuu pitkälti vallitsevien kansainvälisten määritysten pohjalle. Näistä yleisimmällä tasolla on 3GPP:n PWS-dokumentti [2011] Release 11:stä. Se listaa ensin yleiset, globaalit vaatimukset, ja sen jälkeen neljä alueellista, näitä tarkentavaa hanketta: Japanin ETSW:n, Yhdysvaltojen CMAS:n, yhteiseurooppalaisen EU-ALERTin sekä Korean KPAS:n. Näistä EU-ALERTin lisävaatimukset pätevät Suomenkin tapauksessa. Lisäksi määritellään loppukäyttäjän päätelaite (PWS-UE, User Equipment) tarkemmin vielä sellaiseksi, joka pystyy vastaanottamaan varoituksia määritellyllä alueella 3GPP-määritykset toteuttavan verkon välityksellä ja toteuttaa varoitusjärjestelmän määrittelemät toiminnot varoituksen esittämisessä esim. erillisen hälytysäänen avulla. On huomionarvoista, että Suomen oloihin sovellettaessa PWS-UE:n ehto täyttyisi toistaiseksi laajamittaisesti vain perinteisten tekstiviestien avulla.

Yleiset korkean tason vaatimukset varoitusten välittämiselle 3GPP:n mukaan ovat seuraavat:

- Varoitusjärjestelmän tulee pystyä lähettämään varoitusviestejä useille käyttäjille yhtäaikaisesti.
- Useita varoituksia tulee voida lähettää samaan aikaan.
- Varoitukset lähetetään määritellylle alueelle, joka pohjautuu hälytysviestin lähettäjän määrittämään maantieteelliseen alueeseen.
- Varoitusjärjestelmää tukevien päätelaitteiden tulee kyetä vastaanottamaan varoitukset valmiustilassa ollessaan.
- Varoitusjärjestelmän tulee lähettää viestit vain niillä kielillä, joita viranomaisvaatimukset edellyttävät.
- Varoitukset käsitellään siinä järjestyksessä, kun ne saapuvat järjestelmään viranomaisvaatimusten mukaisesti.
- Varoituksen vastaanotto tai näyttäminen käyttäjille ei saa vaatia ennalta olemassa olevaa äänipuhelu- tai datasessiota.
- Varoitukset tulee rajoittaa niihin hätätilanteisiin, joissa ihmishenget tai omaisuus ovat uhattuna ja tilanne vaatii ihmisiltä välittömiä toimenpiteitä.

Varoitusviestien välitysjärjestelmän ei tule itsessään muokata tai kääntää varoitusviestejä toiselle kielelle. Viestien oletetaan sisältävän ainakin seuraavat viisi asiaa:

- Kuvaus tapahtumasta
- Vaikutusalue
- Suositellut toimenpiteet
- Voimassaoloaika (aikavyöhyke huomioiden)
- Viestin lähettänyt viranomainen.

Muuta sisältöä viesteihin voidaan lisätä paikallisten viranomaisvaatimusten mukaisesti. 3GPP:n määritys ei suosita URL-osoitteen tai puhelinnumeron lisäämistä viesteihin lisätietojen saamiseksi. Pelkona on, että mahdollisesti jo ennestään onnettomuudessa vaurioitunut ja hätääntyneiden ihmisten yhteydenotoista kuormittunut matkaviestinverkko ei kestäisi enää äkillistä lisäkuormaa, mikä aiheutuisi viestin vastaanottaneiden ihmisten rynnätessä hakemaan heti lisätietoja.

Aloudat ja Michael [2011] puolestaan esittävät aiempiin tutkimuksiin pohjautuen seuraavan taulukossa 1. kuvatun listan vaatimuksista australialaiselle paikkatietoa hyödyntävälle hätäviestintäjärjestelmälle mobiilipäätelaitteisiin. Olen jakanut karkeasti vaatimukset tyypiltään toiminnallisiksi (**T**) ja/tai laatuvaatimuksiksi (**L**). Monissa kohdin jako ei ole kovin selkeä ja vaatimus voidaan lukea molempiin kategorioihin.

Nro	**Vaatimus**	**Tyyppi**
1.	Järjestelmän tulee olla integroitavissa tai toimittava muiden hälytys- ja varoitusjärjestelmien rinnalla.	T
2.	Järjestelmän on oltava kokonaisuudessaan käytettävissä määrätyille viranomaisille.	T
3.	Ainoastaan määrätyt viranomaiset voivat käyttää järjestelmää viestien lähettämiseen.	T
4.	Järjestelmän on mukauduttava joustavasti tukemaan kaikkia nykyisiä ja tulevia hätätilanteita, eikä se saa olla rajoittunut vain tiettyihin tilanteisiin.	L
5.	Järjestelmä ei saa olla riippuvainen yhden operaattorin verkosta.	T, L
6.	Käytetyn teknologian tulee olla kaikkien maassa toimivien operaattoreiden tukemaa.	L
7.	Järjestelmän tulee olla laajennettavissa uusiin teknologioihin, jotka mahdollistavat tulevaisuudessa laajennettuja siirtotapoja (esimerkiksi suuria datamääriä sisältävät viestit osana varoitusta mm. karttakuvien välitykseen).	L
8.	Järjestelmässä on oltava riittävät suojaukset ja autentikointimekanismit, jotta yksittäisten laitteiden sijaintitiedot voidaan pitää salassa.	L

9.	Järjestelmän tulee tukea sekä ennalta muotoiltuja että dynaamisia viestejä. (T)	T, L
10.	Järjestelmän tulee tavoittaa rajoittamattoman määrä ihmisiä, sadoista harvaan asutuilla alueilla miljooniin kaupungeissa.	L
11.	Siinä on yhtäaikainen viestinvälitys suurelle vastaanottajajoukolle.	T
12.	Viestinvälitys tapahtuu lähes reaaliajassa tai suunnitellun aikajakson sisällä.	T, L
13.	Järjestelmä tavoittaa oikeat vastaanottajat mahdollisimman tehokkaasti hyödyntäen verkkotason teknologiaa vastaanottajien valikointiin sijainnin perusteella.	T, L
14.	Järjestelmä mahdollistaa erilaisten viestien lähettämisen eri vastaanottajajoukoille: esimerkiksi onnettomuuden vaikutusalueella olevia voidaan ohjeistaa yhdellä viestillä ja sinne saapumassa olevia toisella.	T, L
15.	Järjestelmä tavoittaa kaikenlaiset päätelaitteet, mukaan lukien vanhemmat mallit, joita on edelleen runsaasti käytössä.	L
16.	Järjestelmä tukee viestinvälitystä erityisryhmille ja heille optimoiduille laitteille, kuten kuulo- tai näkövammaisille.	T
17.	Järjestelmä tavoittaa myös kaukaisilla alueilla olevat asukkaat sekä vierailijat muista matkaviestinverkoista, mukaan lukien ulkomailta.	T
18.	Järjestelmä tukee viestinvälitystä myös muilla kielillä kuin englanniksi silloin kuin se on mielekästä ja toteutettavissa.	T, L
19.	Järjestelmä kykenee toimittamaan viestin verkon ruuhkatilanteissa.	L
20.	Järjestelmä sisältää toiminnallisuuden viestien uudelleenlähettämiseen, mikäli lähetys epäonnistuu ensimmäisellä kerralla.	T
21.	Viestien toiston tulee olla mahdollista sen voimassaoloaikana.	T

Taulukko 1. Australialaisen hätäviestintäjärjestelmän vaatimukset Aloudatin ja Michaelin [2011] mukaan

Kuten mihin tahansa tietojärjestelmään, myös vaaratiedotteiden välittämiseen sisältyy riskejä ja ongelmakohtia. Erityisesti sellaisia ovat mm. seuraavat Kiddin ja muiden [2008] Uuden-Seelannin viestintäverkojen varoitusteknologista löytämät:

1. **Tiedonsiirtoyhteydet ja kuormituksen huomiointi.** Mikä tahansa vikatilanne tiedonsiirtoverkoissa hankaloittaa varoitusjärjestelmien toimintaa. Esimerkiksi verkkoinfrastruktuurin menetys voi aiheuttaa ruuhkia

verkkoon muuallakin kuin suoraan onnettomuusalueella. Verkot ovat myös ennestään kuormitettuja kriisitilanteissa, jolloin varoituksen lähettäminen lisää itsessään kuormaa, ja edelleen viestin saadessaan vastaanottajat saattavat rynnätä etsimään lisätietoja verkosta.

2. **Optimaalinen hälytyksen aikaikkuna**. Hälytysten välitysnopeus voi riippua verkon kuormituksesta, joka on matalimmillaan yöaikaan. Toisaalta mobiilihälytysten merkitys korostuu tällöin, koska harva seuraa joukkoviestimiä yöaikaan, mutta puhelimen hälytykseen herätään. Perinteiset joukkoviestimet taas tavoittavat kansalaiset parhaiten alkuillasta.
3. **Väestön ohjeistaminen ja sitouttaminen.** Kattava tiedottaminen ja ohjeistaminen ovat ensiarvoisia, jotta väestö saadaan sitoutettua uusien tiedotusjärjestelmien käyttöön (etenkin jos ne vaativat toimenpiteitä loppukäyttäjiltä). Järjestelmän on saavutettava riittävä ”uskottavuus”, jotta varoitusviesteihin reagoidaan asianmukaisella vakavuudella.
4. **Pakollisuus ja valinnaisuus varoituspalvelussa**. Yleisesti ottaen palvelulla, joka käyttäjän pitää itse valita käyttöön, ei saavuteta riittävää kattavuutta. Suurin osa käyttäjistä ei lukuisista syistä ota erikseen palvelua käyttöön ja ohjeistamiseen tarvitaan lisäresursseja. Tavoitettavuuden kannalta pakollinen (automaattisesti aktivoitu) palvelu on huomattavasti parempi, ja käyttäjille voidaan myös tarjota mahdollisuutta erikseen kytkeä se pois päältä.
5. **Varoituksiin väsyminen.** Liian pienistä tapahtumista varoittaminen voi laimentaa varoituksiin reagointia. USAssa tehdyn tutkimuksen mukaan valinnaisen palvelun käyttö lopetetaan melko todennäköisesti varoituksiin väsymisen seurauksena. Samaa päätelmää tukevat Suomessa esitetyt julkiset kommentit [HS, 2010] valtakunnallisista televisiossa välitetyistä vaaratiedotteista.

Yllä esitetyt Aloudatin ja Michaelin vaatimuslista sekä Kiddin ja muiden riskikartoitus ovat pääsääntöisesti linjassa EU-ALERT-hankkeen ja 3GPP:n yleisemmällä tasolla olevan referenssimäärityksen kanssa. Monet Aloudatin ja Michaelin listan kohdista tosin liittyvät ensisijaisesti mobiililaitteisiin välitettäviin sijaintipohjaisiin varoituksiin, mikä muodostaa vain yhden vaaratiedotejärjestelmän alijärjestelmän. Listausta voidaan kuitenkin kokonaisuutena pitää hyvänä lähtökohtana Suomen tarpeisiin sopivan järjestelmän määrittelemiseksi.

5.3. Suomalainen vaaratiedotteiden välitysjärjestelmä

Edellä esitetyn pohjalta luonnostelen nyt erään mahdollisen Suomen oloihin mukautetun vaaratiedotejärjestelmän korkean tason arkkitehtuurisuunnitelman. Järjestelmän käyttötarkoitus on vastaanottaa vaaratiedotteita viranomaisilta ja välittää ne edelleen erilaisiin jakelukanaviin, joiden kautta ne päätyvät mahdollisimman tehokkaasti ja kattavasti määritellylle vastaanottajajoukolle.

Suomen oloihin tarkoitetun järjestelmän toiminalliset vaatimukset on koottu taulukkoon 2.

Kohta	Kuvaus	Huomiot
T01	Järjestelmän tulee pystyä välittämään varoitusviestejä monille käyttäjille samanaikaisesti.	Järjestelmä tavoittaa käyttäjät hierarkkisesti. Suoraan viestialustaan liittyviä asiakasjärjestelmiä voidaan olettaa olevan alle 1000 kappaletta.
T02	Järjestelmä mahdollistaa tiedotteiden välittämisen matkaviestinlaitteisiin.	Viestijärjestelmän alijärjestelmänä on jakelu esim. CBS-tekniikalla.
T03	Varoitusten tulee sisältää seuraavat tiedot: • kuvaus tapahtumasta • vaikutusalue • suositellut toimenpiteet • voimassaoloaika • viestin lähettänyt viranomainen.	Kaikki tiedot ovat mukana CAP-formaatissa. Informaatio voidaan sisällyttää myös *event*-kenttään, jonka sisältö voidaan näyttää TV:ssä ja välittää matkaviestimiin.
T04	Varoitukset lähetetään määritellylle alueelle, joka pohjautuu hälytysviestin lähettäjän määrittämään maantieteelliseen alueeseen.	CAP-viesteissä käytetään *area*-elementtejä kohdealueen määrittelyyn. Tiedon soveltaminen on jakelujärjestelmien vastuulla.
T05	Varoitusjärjestelmän tulee lähettää viestit tarpeen mukaan myös ruotsiksi ja saameksi tiettyjen kuntien alueella sekä tukea muitakin kielivaihtoehtoja (englanti, venäjä).	Yhteen CAP-viestiin voidaan sisällyttää useita erikielisiä *info*-elementtejä.
T06	Varoitukset käsitellään siinä järjestyksessä, kun ne saapuvat järjestelmään.	Viestiväylä toimittaa kaikki viestit vakioajassa vastaanottajille. Jakelujärjestelmien vastuulla on hoitaa viestien toimittaminen.

T07	Järjestelmän kautta lähetetyt viestit voidaan toimittaa samanaikaisesti useiden erilaisten viestikanavien välityksellä.	Televisiohälytykset, tekstiviestit, pelastuslaitosten WWW-sivut ym.
T08	Järjestelmä arkistoi automaattisesti lähetetyt viestit.	Edellytyksenä mm. toiminnolle T09.
T09	Lähetettyä varoitusta voidaan helposti täydentää päivityksillä tai vaara ohi –viestillä.	Sama vastaanottajajoukko on helposti valittavissa päivitettyyn viestiin.

Taulukko 2. Vaaratiedotejärjestelmän toiminnalliset vaatimukset

aulukossa 3 puolestaan on joitakin järjestelmän keskeisiä laatuvaatimuksia. Jälleen rajanveto toiminnallisen ja laatuvaatimuksen välillä on monissa tapauksissa hankalaa. Mikäli järjestelmässä edettäisiin tarkempaan määrittelyyn, laatuvaatimusten huomioonotto konkretisoituisi uusina toiminnallisina vaatimuksina.

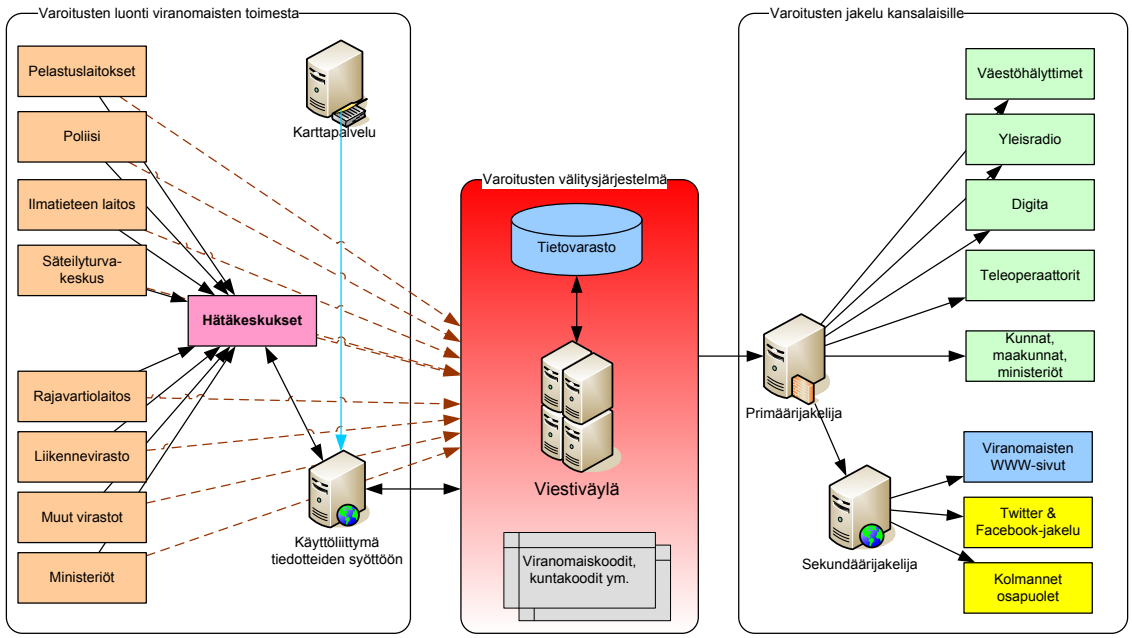
Nro	**Kuvaus**	**Huomiot**
L01	Tiedotteita voivat lähettää vain laissa määrätyt viranomaiset.	Lähetysoikeus varmistetaan henkilökohtaisilla käyttäjätunnuksilla. Käyttöoikeuksien hallinnointi tulee keskittää yhdelle taholle.
L02	Useita varoituksia tulee voida lähettää samaan aikaan.	Viestiväyläarkkitehtuuri skaalautuu helposti suureenkin määrään yhtäaikaisia viestejä.
L03	Järjestelmän kriittiset komponentit on vähintään kahdennettu.	Tietoliikenneyhteyksien kahdentaminen kaikkien viranomaisten järjestelmistä ei todennäköisesti ole mahdollista.
L04	Järjestelmässä käytetään avoimia rajapintoja.	Keskeisin rajapinta ulkoiseen kommunikaatioon on CAP-viestiformaatti. Jakelujärjestelmien sisällä rajapinnat voivat olla suljettuja.
L05	Järjestelmän on tuettava nykyisiä ja tulevia vaaratilanteita, eikä se saa olla rajoittunut vain tietyn tyyppisiin tilanteisiin.	CAP-viestiformaatti on melko joustava.
L06	Järjestelmä tavoittaa oikean vastaanottajajoukon mahdollisimman tehokkaasti hyödyntäen verkkotason teknologiaa vastaanottajien vali-	Liittyy tekstiviestihälytysten toimittamiseen, joka on vaaratiedotejärjestelmän

	kointiin sijainnin perusteella.	alijärjestelmä.
L07	Järjestelmä tavoittaa varoituksen kohdealueella olevat henkilöt riittävän nopeasti.	Viiveen tulisi olla korkeintaan 10 min.

Taulukko 3. Vaaratiedotejärjestelmän laatuvaatimukset

Luonnostelemani vaaratiedotteiden välitysjärjestelmä koostuu CAP-muotoisia viestejä kuljettavasta viestiväylästä, joka toteuttaa julkaisija-tilaaja (publish-subscribe) viestinvälitysparadigman. Viranomaiset ovat viestien julkaisijoita, jotka lähettävät viestit nimettyyn viestikanavaan, jota puolestaan tilaavat erilaiset viestien välitysjärjestelmät jakelijarajapinnan kautta. Järjestelmä muistuttaa rakenteeltaan paljon IPAWS-järjestelmää, mutta olen tehnyt siihen joitakin lisäyksiä ja tarkennuksia.

Vaaratiedotejärjestelmän ja siihen liittyvien järjestelmien kokonaisarkkitehtuurikuva on esitetty kuvassa 16.



Kuva 16. Vaaratiedotejärjestelmä ja sen keskeiset liitännät

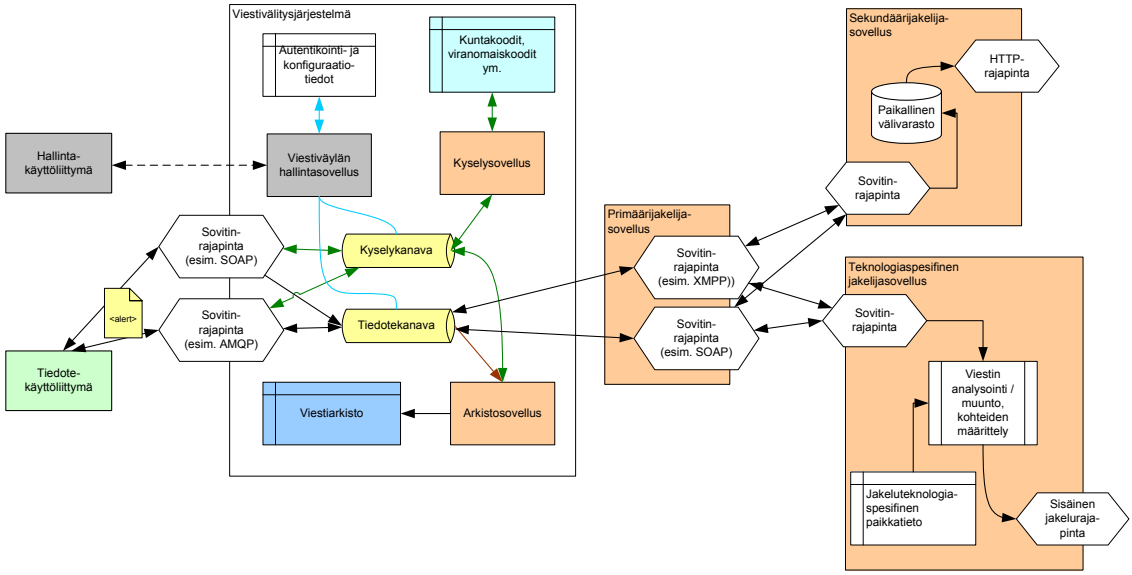
Palvelun ytimenä on varsinainen varoitusten välitysjärjestelmä, joka koostuu viestiväyläsovelluksesta, tietoarkistosta, CAP-viestien rikastamista tukevasta koodistosta sekä näitä palvelevista oheissovelluksista. Järjestelmään voidaan katsoa kuuluvaksi myös yksinkertainen viranomaisten jaetussa käytössä oleva tiedotteiden syöttökäyttöliittymä sekä tiedotteet eri rajapintatekniikoilla jakeleva primäärijakelija. Nämä on kuvassa 16 esitetty erillisinä palvelinkomponentteina loogisen jaottelun sekä tietoturvarajojen vuoksi, mutta periaatteessa ne on mahdollista myös integroida samaan yhteiseen alustatoteutukseen. Kuva 16 ei

ota kantaa redundanttiin toteutukseen, mutta lähtökohtaisesti ainakin viestiväyläsovellus ja tiedotteiden jakelija tulisi kahdentaa, mieluusti täysin erillisillä infrastruktuuritoteutuksilla (palvelinalustat, konesalit, sähkönsyöttö, tietoliikenneyhteydet). Ytimenä oleva viestiväyläsovellus tulee valita siten, että se tukee itsessään varmistavaa tai klusteritoteutusta, jolloin mahdollisen klusterinoodin vikaantuminen ei kadota tietoja tai aiheuta merkittävää (>5 min) katkosta tiedonsiirtoon.

Viestien jakelu on hajautettu kahteen tasoon, joista ensimmäisessä primäärijakelija toimii rajapintamuunnokset ja autentikoinnit tekevänä välityspalvelimena (suojaten samalla varsinaisen viestialustan infrastruktuuria olemalla sen edessä) tärkeimmille järjestelmän asiakkaille. Näitä ovat varsinaiset varoitukset lähettävät organisaatiot ja niiden tietojärjestelmät. Ne liittyvät primäärijakelijan rajapinnan kautta tilaajiksi viestiväylälle, jolloin sinne julkaistu tiedoteviesti jaetaan automaattisesti kaikille. Viestialusta huolehtii mahdollisesta viestin jonouttamisesta ja automaattisesta uudelleenlähetyksestä, mikäli yhteys jostakin syystä on katkennut. Vastaanottavien sovellusten vastuulla on tarkastella CAP-viestin sisällön perusteella, onko se voimassa ja validi toimitettavaksi eteenpäin. Toteutus ei ota juurikaan kantaa siihen, miten CAP-viestin saatuaan kukin organisaatio muovaa viestin sisällön omiin jakelukanaviinsa sopivaksi, mutta lähtökohtaisesti jokaisen vastaanottavan järjestelmän tulisi tarkastaa viestin oikeellisuus ja tehdä *area*-elementtien perusteella päätelmät siitä, miten viesti kohdistetaan alueellisesti jakelijan omassa infrastruktuurissa. Esimerkiksi teleoperaattoreiden tulisi valita jakeluun kaikki ne tukiasemat verkostaan, jotka sijaitsevat CAP-viestissä määritellyllä alueella.

Sekundäärijakelija puolestaan on yksi asiakasohjelma, joka tarjoaa CAP-tiedotteet laajempaan julkiseen käyttöön kolmansien osapuolten palveluihin (esim. sosiaalisen median julkaisusovellukset). Eriyttämällä nämä omaan palveluunsa parannetaan varsinaisen vaaratiedotejärjestelmän tietoturvaa ja estetään suorituskykyongelmia.

Olen edelleen luonnostellut tarkemman esimerkkikuvauksen vaaratiedotejärjestelmän keskeisten osien sisäisestä arkkitehtuurista (Kuva 17). On kuitenkin huomioitava, että yksityiskohtaisempi toteutus riippuu monista järjestelmän suunnitteluvaiheessa tehtävistä valinnoista (valmiiden komponenttien käyttö, ohjelmointikielet, viestinvälitysarkkitehtuuri, monitoimittajaympäristö ym.), joten tässä esitetty on vain eräs mahdollinen vaihtoehto toteutukselle.



Kuva 17. Vaaratiedotejärjestelmän sisäinen arkkitehtuuri

Viestivälitysjärjestelmään on tässä esitetty kaksi kanavaa, joista toinen on varsinainen CAP-sanomien välitykseen käytetty julkaisija/tilaaja -kanava, ja toinen taas tukitoimintoja tarjoava kysely- ja arkistosovelluksien käytössä oleva, jonka kautta asiakasjärjestelmät voivat noutaa erikseen määriteltävän sanomaformaatin avulla tietoja kunta- ja viranomaiskoodistosta tai arkistoituja CAP-viestejä. Kuvassa 17 on esitetty esimerkkeinä muutamia erilaisia tavanomaisimpia viestiväyläarkkitehtuuriin soveltuvia rajapintoja ja niille sovittimia. On myös mahdollista, että asiakassovellukset liittyvät suoraan viestiväylän natiivilla toteutuksella (esimerkiksi JMS) kiinni väylään ilman sovittimia. Viestivälitysjärjestelmän sisällä kaikki tietovirrat on kuvattu kaksisuuntaisiksi, koska vaikka varsinaiset CAP-viestit liikkuvat ensisijaisesti vain yhteen suuntaan, viestiväylän kehysprotokollan tulee mahdollistaa myös kuittausviestit toiseen suuntaan.

5.3.1. Vaaratiedoteviestin muoto

Vaaratiedotejärjestelmän välittämät viestit ovat vakiomuotoisia ja sisältävät aina vähintään jokaiselle viestille pakolliset perustiedot sekä valinnaisesti muitakin tietoja. Viestiformaatin on mielekästä pohjautua kansainvälisesti käytettyyn OASIS-järjestön määrittelemään EDXL-CAP-muotoon (Emergency Data Exchange Language - Common Alerting Protocol), josta myös televiestintäjärjestö ITU-T [2008] on luonut standardin X.1303. Rakenteellinen CAP-viesti koostuu *alert*-juurielementistä, joka sisältää perustiedot hälytyksestä. Tämän alla voi olla yksi tai useampia *info*-elementtejä, jotka sisältävät tarkemmat tiedot (esim. varoitusviesti eri kielillä). Edelleen jokaista info-elementtiä voi tarkentaa yksi tai useampi *resource*-elementti, joka määrittää liitetiedoston (esim. varoitusviesti

audiomuodossa), sekä yksi tai useampi *area*-elementti, joka määrittää varoituksen maantieteellisen kohdealueen. ITU-T:n määritys sisältää sekä XML-enkoodauksen että vastaavan binäärimuotoisen ASN.1 -määrityksen.

Esimerkki EDXL-CAP v1.1:n mukaisesta sanomasta XML-muodossa on esitetty liitteessä 1. CAP-formaattiin pohjautuen on jo käytössä paikallisia tarpeita vastaavat viestiprofiilit Yhdysvalloissa (CAP-IPAWS) sekä Australiassa (CAP-AU-STD). Näihin pohjautuen esitän taulukossa 4 luonnoksen ”CAP-FI”-formaatista Suomen vaaratiedotteita varten. Lihavoidut elementit ovat pakollisia, tähdellä merkityt voivat CAP-määrityksen mukaan esiintyä viestissä useita kertoja. Taulukosta on jätetty pois juurielementti *alert*, jonka sisään muut elementit kuuluvat.

CAP-elementti	Käyttökuvaus	Lisähuomiot
identifier	Yksikäsitteinen tunniste viestille.	CAP-määrityksen mukaan lähettäjän määrittämä, mutta voidaan käytännössä luoda vaaratiedotejärjestelmässä kun uusi viesti vastaanotetaan.
sender	Viestin lähettäjän yksikäsitteinen tunniste.	Lähettäjiä varten voidaan määritellä vakiomuotoinen hierarkkinen esitystapa, esim. ”FI.ERC.TURKU” tarkoittaisi Varsinais-Suomen hätäkeskusta. Tällä avaimella voidaan ulkopuolisesta järjestelmästä hakea viranomaisen tarkemmat yhteystiedot sekä nimet eri kielillä.
sent	Aikaleima, jolloin viesti on lähetetty. Kaikki aikaleimat ovat UTC-muodossa sisältäen aikavyöhykkeen.	Mikäli viesti halutaan julkaista vasta myöhemmin, voidaan käyttää *onset* -kenttää.
status	ITU-T määrittää seuraavat: ”Actual” – todellinen tiedote ”Exercise” – harjoitusviesti, lisätietoja *note* -elementissä. ”System” – järjestelmän sisäiseen viestinvälitykseen ”Test” – Tekninen testiviesti, tulee jättää huomiotta. ”Draft” – Luonnos, ei aiheuta vielä toimenpiteitä.	Kaikkien vastaanottajien on tuettava ainakin ”Actual” -tyyppisiä viestejä.

msgType	ITU-T määrittää seuraavat: ”Alert” – ensimmäinen viesti uudesta varoituksesta ”Update” – päivittää ja täydentää aiempia viestejä, joiden tunnisteet *references*-elementissä. ”Cancel” – peruuttaa aiemmat viestit (*references*) ”Ack” – kuittaus vastaanotosta (*references*) ”Error” – virhekuittaus, tarkempi tieto *note*-elementissä (references)	Kuittausviestejä voidaan käyttää joidenkin tärkeimpien vastaanottajien osalta (Yleisradio, Digita, teleoperaattorit). Pääosin vastaanottajien tulisi jättää ne huomiotta.
source	Mikäli hätäkeskus lähettää toisen viranomaisen puolesta viestin, tällä voidaan kertoa alkuperäinen lähettäjä.	*sender* on aina viestin teknisesti lähettänyt taho. Ks. myös *senderName*
scope	ITU-T määrittää seuraavat: ”Public” – julkinen vaaratiedote ”Restricted” – rajoitetulle joukolle lähetetty, määritelty tarkemmin *restriction*-elementissä. ”Private” – ainoastaan *address*-elementissä määrätyille vastaanottajille.	Suomen oloissa järjestelmää käytettäneen ensisijaisesti vain julkisten viestien välittämiseen. Restricted -tyyppiä voitaisiin kuitenkin hyödyntää rajaamaan viesti vain tiettyihin jakelutyyppeihin, esim. ”DVB”-määrityksellä viesti näytettäisiin vain televisiossa. Tähän voidaan käyttää myös *parameter*-elementtejä.
restriction	Käytetään, jos *scope* on ”Restricted”.	
addresses	Käytetään, jos *scope* on ”Private”.	Vastaanottajan rajaus lähinnä testitapauksissa. Esimerkiksi ”FI.MNO.ELISA” yhdessä *status* = ”Test” kanssa vain Elisalle lähetyssä testissä.
code *	Viestiformaatin versio. Esimerkiksi CAP-FI-1.2	
note	Käytetään lähinnä Cancel- ja Error-tyyppisten viestien kanssa.	Vapaateksti viestin peruutuksen syystä.
references	Mikäli viesti päivittää aiemmin annettua varoitusta tai peruuttaa sen, yksilöivät viittaukset aiemmin annettuihin varoituksiin.	ITU-T:n mukaan viesti identifioidaan kolmen kentän yhdistelmällä (*sender, identifier, sent*). Käytännössä *identifier* pitäisi olla riittävä.
incidents	Mikäli samasta tapahtumasta on	Pääsääntöisesti käytäntönä

		annettu useita erityyppisiä varoituksia, listataan tässä muiden yksilöivät tunnisteet.	lienee antaa aiempaa varoitusta täydentäviä viestejä, ei useita erillisiä varoituksia.
info *		Varoituksen viestisisällön ryhmityselementti.	Useita info-elementtejä voidaan käyttää varoituksen esittämiseen eri kielillä
	language	Varoituksen kieli.	IETF RFC3066:n kielikoodilla, esim: ”fi-FI”, ”fi-SV” tai ”smn” (inarinsaame)
	category	Tapahtuman luokitus. ITU-T määrittää: "Geo" – esim. maanvyörymä "Met" – esim. voimakas myrsky "Safety" – yleinen vaaratiedote "Security" – poliisitiedote "Rescue" – pelastustiedote "Fire" – palontorjunta ja pelastus "Health" – terveystiedote "Env" – myrkkypäästöt ja muut ympäristövaarat "Transport" – kulkuneuvot ja liikenne "Infra" – infrastruktuuri (muu kuin liikenne) "CBRNE" – kemiallisen, biologisen, radioaktiivisen tai räjähdeaseen uhka tai hyökkäys "Other" – muut tilanteet	Suomessa lienee helpointa käyttää aluksi “Safety”-tyyppiä kaikkiin tiedotteisiin.
	event	Varoitusviesti. Tärkein viestisisältö, joka välitetään kaikkiin viestikanaviin.	Kentän pituuden tulee olla rajattu lyhimmän teknisen rajoitteen mukaan (esim. tekstiviestin pituus). Avainsisältö oltava aina tässä, vaikka elementtejä *responseType, headline, description* ja *instruction* käytettäisiinkin tarkentamaan ohjeita.
	responseType	Toimintaohje varoitukseen liittyen, tarkennus *instruction*-elementissä. ITU-T määrittää: ”Shelter” – siirry väestönsuojaan ”Evacuate” – siirry pois alueelta ”Prepare” – valmistaudu ”Execute” – suorita ennalta määritelty toimenpide ”Monitor” – seuraa tiedotuksia	Ensisijaisesti kaikki toimintaohjeet välitetään *event*-elementissä.

		”Assess” – arvioi viestin sisältö (ei tule käyttää julkisissa varoituksissa) ”None” – ei vaadi toimenpiteitä.	
	urgency	ITU-T määrittää viisi tasoa liittyen siihen, milloin vastaanottajan tulisi reagoida varoitukseen: ”Immediate”, ”Expected”, “Future”, “Past”, “Unknown”	Ohjeistus ensisijaisesti *event*-kentässä.
	severity	ITU-T määrittää viisi tasoa tapahtuman vakavuudelle: ”Extreme”, ”Severe”, ”Moderate”, ”Minor”, ”Unknown”.	Ohjeistus ensisijaisesti *event*-kentässä.
	certainty	ITU-T määrittää viisi tasoa tapahtuman todennäköisyydelle: ”Observed”, ”Likely”, ”Possible”, ”Unlikely”, ”Unknown”.	Ohjeistus ensisijaisesti *event*-kentässä. ”Likely” tarkoittaa yli 50% todennäköisyyttä, ”Possible” 50% tai alle. CAP 1.0-versiossa myös ”Very Likely”, joka tulee tulkita kuin ”Likely”.
	audience	Varoituksen kohderyhmä.	Ei liene syytä käyttää, oletusarvoisesti kaikki *area*-elementissä määritellyllä alueella olevat.
	eventCode *	Tapahtuman tyyppi.	Esimerkiksi ”VAARATIEDOTE”, ”MUU VIRANOMAISTIEDOTE”, ”HÄTÄNUMEROTIEDOTE” mutta voidaan laajentaa eriasteisiksi järjestelmän käytön lisääntyessä.
	effective	Aikaleima, varoitus voidaan välittää joissakin tapauksissa jo ennen sen julkaisuaikaa.	Mikäli elementtiä ei ole mukana, viestin oletetaan olevan julkaistavissa välittömästi.
	onset	Aikaleima, jolloin varoituksessa ilmoitettu tapahtuma alkaa.	Esim. myrskyvaroituksissa asiasisältö jo *event*-elementissä.
	expires	Aikaleima, jolloin varoituksen voimassaolo päätty.	Varoituksille tulee asettaa esim. 24 tunnin oletusvoimassaoloaika.
	senderName	Varoituksen antanut viranomainen *info*-elementin mukaisella kielellä.	Esimerkiksi ”Varsinais-Suomen hätäkeskus”, ”Egentliga Finlands nödcentral”
	headline	Tapahtuman otsikko. Pääsäntöisesti sama kuin *event*.	Ensisijaisesti käytetään elementtiä *event* viestisisältöön. Rakenteellisia kenttiä *respon-*
	description	Tarkempi kuvaus tapahtumasta.	

	instruction	Erillisiä toimintaohjeita.	*seType, headline, description, instruction, web* ja *contact* tulee käyttää vain, mikäli varoitusviesti välitetään nämä elementit ymmärtävään palveluun (esim. WWW-sivut).
	web	URL-osoite lisätietoja varten.	Mikäli viestissä annetaan lisätieto-osoite, sen takana olevan verkkopalvelun tulee kestää äkillinen kuormituspiikki.
	contact	Puhelinnumero lisätietoja varten.	Käyttö vain pienelle vastaanottajajoukolle lähetetyissä viesteissä, jotta vältetään viestiverkkojen ylikuormitusta.
	parameter *	Voidaan käyttää lisätietojen välittämiseen.	Parametreilla voidaan laajentaa viestiä, määrittelemällä esim. toistofrekvenssi.
	resource *	Viestiin voidaan määrittää mukaan myös liitetiedostoina esimerkiksi karttakuvia tai ääni- tai videonauhoite toimintaohjeista.	Mahdollisten ääni- tai videonauhoitteiden tulisi sisältää sama varoitusinformaatio kuin tekstimuotoisenkin viestin.
		resourceDesc	Kuvaus liitteen tyypistä.	Esimerkiksi ”Karttakuva alueesta”
		mimeType	Esimerkiksi ”audio/mpeg”.	IETF RFC 2046:n mukaan.
		size	Liitetiedoston koko tavuina.	
		uri	URL-osoite, josta vastaanottavat järjestelmät voivat noutaa liitteen.	Vastaanottajilla tulee olla pääsy osoitteeseen. Järjestelmän tulee kestää yhtäaikaisten hakujen äkillinen määrä. Julkisen levityksen kohdalla sekundäärijakelijan tulee kopioida tiedosto välimuistiin ja muuttaa uri vastaamaan tämän osoitetta.
		deferUri	Vaihtoehto *uri*-elementille. Voi sisältää liitetiedoston base64-muotoisena, mikäli vastaanottava järjestelmä ei pysty noutamaan URL-osoitteesta viestiä.	Käyttö mahdollista lähinnä audiopohjaisten väestöhälytimien yhteydessä. Lisää kuormitusta viestiväylällä ja sen tietoliikenneyhteyksillä.
		digest	SHA-256 tiiviste liitetiedostosta, jonka avulla vastaanottaja voi varmistua sen eheydestä.	
	area *		Varoituksen kohdealueen määrittävä ryhmittelyelementti.	

			Viestissä voi olla useita “area” -elementtejä.	
		areaDesc	Tekstimuotoinen kuvaus alueesta.	Voidaan käyttää esimerkiksi samaa jakoa, kuin Ilmatieteen laitoksen varoituksissa. Kohdennettujen varoitusten osalta tarkempi määrittely *geocode*-elementissä on oltava mukana.
		polygon *	Pituus- ja leveysasteparien lista, jotka määrittävät vaikutusalueen reunapisteet kartalla.	Koordinantit WGS 84 -standardin mukaan. Yksi *area*-elementti voi sisältää useita *polygon*- tai *circle*-elementtejä.
		circle *	Pituus- ja leveyspari sekä kilometriarvo, jotka määrittävät ympyrän muotoisen vaikutusalueen.	Koordinantit WGS 84 -standardin mukaan.
		geocode *	Sisältää kansallisesti määriteltyjä aluekoodeja *valueName* – *value* -elementtien pareina.	Tarkemmin määriteltävä hierarkkinen toteutus eri *valueName*-attribuuteilla. Näissä on syytä käyttää vakiintuneita luokitteluja, esim. ISO 3166-2:FI yksilöi maakunnat, JHS 110 taas kuntakoodit.
		altitude	Varoituksen korkeustieto, jalkoina merenpinnasta.	Ei liene tarpeellinen Suomen oloissa.
		ceiling	Varoituksen lakikorkeus, jalkoina merenpinnasta.	Ei liene tarpeellinen Suomen oloissa.

Taulukko 4. Esimerkki CAP-viestiprofiilista Suomen vaaratiedotteiden välittämiseen

Lähtökohtaisesti kaikki viestit välitetään järjestelmässä UTF-8 -enkoodattuina XML-muodossa. Vastaanottavien järjestelmien tulee tarpeen mukaan muuntaa viestit (karsien epäolennaiset ja ei-tuetut elementit) omaan sisäiseen viestimuotoonsa. Vaaratiedotejärjestelmään kuuluu viestinvälitysalustan lisäksi myös tietovarasto, jossa säilytetään arkistoidut kopiot kaikista järjestelmän välittämistä viesteistä. Samaan tapahtumaan liittyvät viestit ryhmitellään nk. tapahtumakansioihin, jolloin ne ovat helposti tarkasteltavissa esimerkiksi luotaessa uutta päivitystiedotetta tapahtumasta.

5.3.2. Viranomaisten liitännät järjestelmään ja yhteydet muihin järjestelmiin

Vaaratiedotejärjestelmän monipuoliset rajapinnat mahdollistavat erilaiset liitännät viranomaisten järjestelmiin joustavasti. Yksinkertaisimmillaan tiedotteita antavat viranomaiset voivat käyttää esimerkiksi WWW-selaimella toimivaa käyttöliittymää. Avoimet rajapinnat mahdollistavat myös tiedotejärjestelmän integroinnin suoraan muihinkin viranomaisten järjestelmiin, esimerkiksi Säteilyturvakeskuksen mittalaiteverkostoon tai Ilmatieteen laitoksen järjestelmiin. Näiden avulla järjestelmää on tulevaisuudessa mahdollista laajentaa välittämään erilaisia automatisoituja varoitusviestejä suoraan näidenkin viranomaisten järjestelmistä.

Järjestelmän yleisimmässä käyttötapauksessa vaaratiedotteen syöttää järjestelmään hätäkeskuksen päivystäjä käyttäen järjestelmän omaa käyttöliittymää, joka voidaan toteuttaa esim. www-selaimessa toimivana. Tiedotekäyttöliittymään pääsy on tietoturvasyistä tiukasti rajattu toimimaan vain salattujen yhteyksien yli viranomaisverkoista ja jokainen käyttäjä tulee autentikoida erikseen. Käyttöliittymällä syötetään tiedotteen perustiedot (tärkeimpänä tiedoteteksti *event*), valitaan kohdealue joko karttanäkymältä tai vaihtoehtoisesti esimerkiksi listanäkymästä (jossa kohdealueeksi voidaan ottaa yksi tai useampi kunta tai maakunta) ja lopuksi lähetetään tiedote järjestelmään, joka hoitaa automaattisesti sen jakelun eteenpäin. Saman käyttöliittymän kautta voidaan päivittää aiemmin annettuja tiedotteita ja mahdollisesti suorittaa järjestelmään liittyvien kunta- ja virainomaiskoodien sekä karttamateriaalin ylläpitoa.

Vaaratiedotejärjestelmä itsessään ei välttämättä tarvitse suoraan tietoa muista viranomaisjärjestelmistä. Monet vaaratiedotteiden antamisen tukena olevat järjestelmät (mm. sääennusteet, pelastustoimen ja poliisin tehtävätiedot) ovat todennäköisesti käytettävissä hätäkeskuksissa jo entuudestaan näiden omien käyttöliittymien avulla ja niiden integrointi suoraan vielä vaaratiedotejärjestelmään monimutkaistaisi sen toteutusta. Toisaalta, mikäli integrointi onnistuu helposti (esim. upottamalla sisältöelementtejä tiedotejärjestelmän WWW-käyttöliittymään portaalimaisesti), järjestelmän käytettävyys saattaisi parantua.

Paikkatietojärjestelmän integrointi ainakin tiedotteiden antojärjestelmään sen sijaan on mielekästä, jolloin tiedotteen vaikutusalue voidaan valita suoraan karttanäkymästä. Varsinaisissa tiedoteviesteissä paikkatieto sen sijaan välitetään vain joukkona koordinaatteja tiedotteen metatiedoissa, jolloin vastaanottavien järjestelmien tehtävänä on soveltaa näitä koordinaattietoja omiin tarpeisiinsa (esim. teleoperaattorin verkon solujen vastaavuus valittuun maantieteelliseen alueeseen). Vastaavasti järjestelmässä on mielekästä pitää keskitetysti yl-

lä tietokantaa tiedotteissa käytettävistä koodiarvoista ja niiden selväkielisistä vastineista ja muista tiedoista (esim. viranomaisten nimet ja yhteystiedot, kielikoodit, kuntakoodit). Näiden kyselyyn (ja muokkaukseen) tarjotaan yksinkertaiset rajapinnat.

5.4. Tiedotteiden välitys kansalaisille

Seuraavissa alikohdissa kuvaan teknologioita viestien toimittamiseen perille vaaratiedotejärjestelmässä. Myös perinteiset väestöhälyttimet ovat osa välitysjärjestelmää. Nekin tulisi liittää CAP-yhteensopivalla rajapinnalla vaaratiedotejärjestelmään siten, että annettu tiedote toistetaan automaattisesti myös väestöhälyttimillä.

5.4.1. TV:n ja radion kautta välitettävät varoitukset

Nykytilanne, jossa kaikki vaaratiedotteet välitetään TV-lähetysten kautta koko valtakunnan alueelle, on tiedotteiden uskottavuuden ja järjestelmän merkityksellisyyden kannalta ongelmallinen. TV-lähetyksiä katkovat useimmille vastaanottajille täysin epärelevantit tiedotteet ärsyttävät vastaanottajia ja nostavat kynnystä käyttää TV:tä vaaratiedottamisen kanavana.

TV:n kautta välitettävät tiedotteet tulisi rajata nykyistä paremmin alueellisiksi ja varmistua siitä, että tiedotteet pakkosyötetään kaikille kanaville jakelutekniikasta (maanpäällinen, kaapeli, internet) riippumatta. Satelliittijakelu muodostaa poikkeuksen, sillä ei ole realistista olettaa, että monien valtioiden alueelle kohdistuviin lähetyksiin, joiden jakelijayritykset sijaitsevat ulkomailla, saataisiin mukaan suomalaiset tiedotteet). Toteutus tulee sisällyttää edellytykseksi TV-lähetysten jakeluun esimerkiksi Viestintämarkkinalain muutoksella ja Viestintäviraston määräyksillä, kuten nykyisellääänkin on säädetty hätätiedotteiden välittämisestä radioverkkoa käyttävien joukkoviestimien osalta.

Mikäli tiedotteiden rajaaminen alueellisesti TV-jakelussa ei onnistu, tulee harkita tämän jakelukanavan käyttöä ainoastaan äärimmäisen merkittävissä vaaratilanteissa, joissa uhan vaikutusalueella on tuhansia ihmisiä, tai uhka voi liikkua nopeasti alueelta toiselle.

5.4.2. Tekstiviesti- ja CBS-varoitukset

Mobiilipäätelaitteisiin toimitettavat hälytykset lienevät paras tapa kansalaisten varoittamiseen nykypäivänä, joten niiden viestimahdollisuuksien hyödyntäminen tulee olla yksi keskeisimpiä kohtia vaaratiedotejärjestelmässä. Toisaalta sen toteutus ei kuitenkaan saisi muodostua kynnyskysymykseksi muulle järjestelmälle, kuten toistaiseksi Suomessa on vaikuttanut tilanne olevan. Vakioidun varoitusviestiformaatin ja avointen rajapintojen myötä varoitusjärjestelmään

voidaan liittää uusia viestinvälitysjärjestelmiä olemassa olevien rinnalle myöhemminkin, ja toisaalta olemassa olevia järjestelmiä on helppo päivittää.

Tekstiviestihälytysten teknistä toteutusta ja siihen liittyviä ongelmia olen käsitellyt laajasti edellisessä luvussa. Keskeinen haaste on, että normaalien tekstiviestien tapauksessa pitää ennen viestin lähetystä tietää vastaanottajien MSISDN-numerot. Näiden kerääminen tietyllä maantieteellisellä alueella olevilta verkon käyttäjiltä on teknisesti vaikea ja hidas operaatio, jota nopeuttavat ratkaisut vaatisivat lisäinvestointeja operaattoreiden verkkoihin. Toisaalta taas CBS-tekniikan käyttö varoituksiin näyttäisi olevan kansainvälisesti valittu kehityssuunta useassa eri maassa ja projektissa, joten se tulisi ehdottomasti ottaa käyttöön Suomessakin. Periaatteessa olisi mahdollista käyttää molempia teknologioita rinnakkain, mutta käyttöönottoon kuluvan ajan ja investointikustannusten vuoksi tämä ei ole mielekäs vaihtoehto.

5.4.3. Mobiilidataliikenteen pakko-ohjaus tiedotesivulle

Yhä suurempi osa matkapuhelinverkon käytöstä etenkin 3G- ja 4G-verkoissa on mobiilidataliikennettä. Vaikka käyttäjien päätelaitteissa onkin samanlainen SIM-kortti kuin perinteisissä matkapuhelimissa ja tällä edelleen tekninen MSISDN-numero, ei laite välttämättä pysty vastaanottamaan perinteisiä SMS-tekstiviestejä. Esimerkiksi suositulla Applen iPad-taulutietokoneella ei pysty ilman erityisohjelmistoja vastaanottamaan tai lähettämään tekstiviestejä. Monet operaattorit (toistaiseksi kuitenkin vain Suomen ulkopuolella) myös markkinoivat tällaisiin laitteisiin pelkästään pakettidatakäytön mahdollistavia liittymiä, jolloin tekstiviestien tai puheluiden vastaanotto ei ole mahdollista verkonkaan puolesta.

Pakettidatayhteyksille on kuitenkin teknisesti mahdollista operaattorin toimesta pakottaa tietyn tyyppinen liikenne tilapäisesti operaattorin valitsemalle tiedotussivulle. Käytännössä mobiilidataverkon ja internetin välissä oleva verkkoelementti (esim. GGSN tai erillinen läpinäkyvä IP-välityspalvelin) tunnistaa ja kaappaa käyttäjän HTTP-session ja ohjaa sen käyttäjän syöttämän URL-osoitteen sijaan operaattorin määrittelemälle sivulle. Uudelleenohjaus voidaan poistaa esimerkiksi ensimmäisen ohjauskerran jälkeen, tai se voidaan tehdä jatkuvasti kaikille käyttäjän avaamille HTTP-istunnoille kunnes operaattori kytkee toiminnon pois päältä.

HTTP-sessioiden pakko-ohjaus olisi teknisesti helppo toteuttaa nykyisten mobiiliverkkojen ja Internetin reunalle. Tiedotesivulla näytettävä viesti olisi sisällöltään sama hätätiedoteteksti, mikä välitettäisiin muidenkin kanavien kautta, mutta verkkosivulle olisi mahdollista linkittää heti sen yhteyteen erilaisia

yleispäteviä toimintaohjeita erilaisiin vaaratilanteisiin sekä viranomaisten verkkosivuja.

5.4.4. Tiedottaminen viranomaisten verkkopalveluissa

Vaaratilanteissa viranomaisten verkkopalvelujen (WWW-sivujen) merkitys tiedotuskanavana korostuu. Vaikka kansalaiset todennäköisesti saavatkin ensimmäisenä tiedon tapahtumasta jonkin muun kanavan (joukkoviestimet, vaaratiedotteet) kautta, verkkopalvelu on looginen paikka etsiä lisätietoa asiasta. Etenkin jos julkisuuteen annetaan tiedote, että asiasta on lisätietoja viranomaisen verkkopalvelussa (kuten esim. Aasian tsunamikatastrofin yhteydessä vuodenvaihteessa 2004–2005), palvelun tulisi myös tarjota nämä tiedot ja olla tavoitettavissa yllättävästä kuormituspiikistä huolimatta.

Kuntaliiton verkkoviestintäohjeistuksessa [Kuntaliitto, 2010] määritellään seuraavat minimivaatimukset poikkeus- ja kriisioloissa käytettävälle kunnan kriisiviestintäsivustolle:

- Kuntalaisia koskevat määräykset, ohjeet ja suositukset kriisitilanteessa.
- Lisätietojen antajat: Kunnan osalta niiden henkilöiden yhteystiedot, jotka vastaavat tiedusteluihin, muiden viranomaisten osalta tarpeelliset yhteystiedot esimerkiksi henkilötiedustelujen osalta.
- Kriisiavun yhteystiedot.
- Linkit muiden viranomaisten sivuille. Perusperiaate on, että jokainen viranomainen hoitaa verkkotiedotuksen omien käytäntöjensä mukaan eli yhteisiä kriisiportaaleja ei luoda.
- Tiedotteet tarkalla kellonajalla ja päivämäärällä varustettuna.
- Tiedotustilaisuuksien ajankohdat.
- Asukkaille suunnattujen tilaisuuksien ajankohdat.
- Linkki kunnan perussivuille. Tieto kriisistä tulee myös lisätä kunnan perussivuille sekä samalla kertoa kriisin mahdollisista vaikutuksista perussivujen toimintaan.
- Jos kunta on esillä organisaationa sosiaalisen median palveluissa, olisi näihin käytävä ainakin päivittämässä linkki kunnan kriisisivustolle.

Osittain tätä kuntien tarpeeseen tehtyä listaa täydentäen määrittelen yleisesti viranomaisten verkkopalvelulle seuraavan listan vähimmäisvaatimuksista, mitkä niiden pitäisi täyttää sellaisissa poikkeustilanteissa, joissa väestöä on varoitettu vaaratiedotteella:

1. Verkkopalvelun etusivulla tulisi olla välittömästi selkeästi esillä sama hätätiedoteviesti, joka on välitetty muidenkin kanavien kautta. Mikäli hätäviestit olisivat saatavilla vakiomuotoisina rajatun käyttäjäjoukon verkkopalvelussa, näiden automaattinen nouto ja esittäminen alueellis-

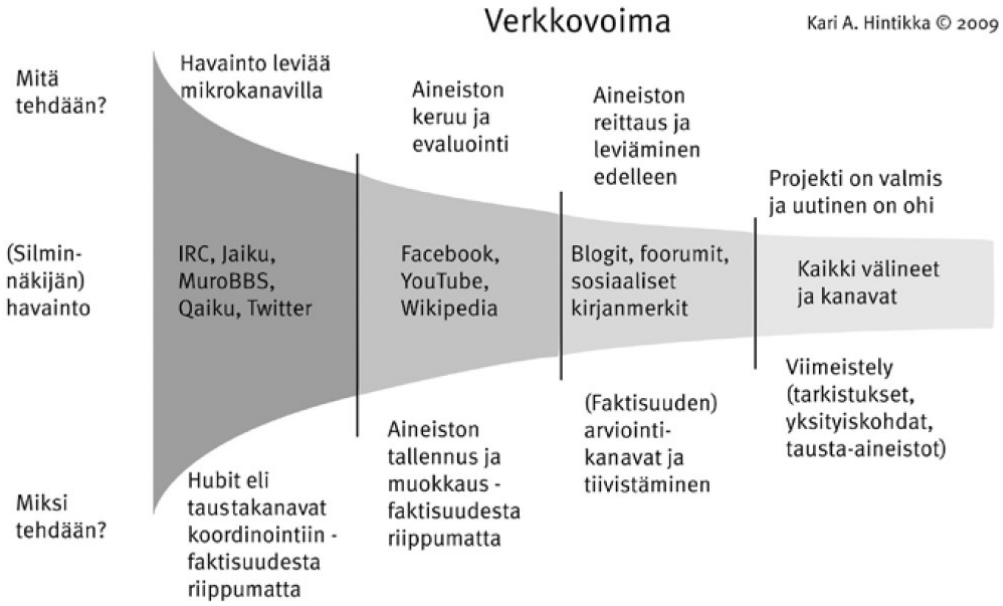
ten poliisi- ja pelastusviranomaisten verkkosivuilla olisi yksinkertaista toteuttaa.

2. Tiedotetta tulisi täydentää lisäohjeilla, kartoilla, yhteystiedoilla ym. Pitkäkestoisen tilanteen yhteydessä sivuille tulisi luoda oma erikoisosionsa tapahtumaan liittyvälle tiedottamiselle.
3. Verkkopalvelun tulee kestää poikkeava kuormituspiikki, joka aiheutuu vaaratilanteessa tiedottamisesta. Myöskään muut osat verkkopalvelusta eivät saa olla tavoittamattomissa kuormituspiikin aikana, koska samaa verkkopalvelua saatetaan käyttää myös laajamittaisesti normaaliin asiointiin. Korkean käytettävyyden palveluiden toteutusta on kuvattu tarkemmin alakohdassa 3.4.4.

Poikkeusoloihin varautuminen muodostaa myös hyvän pohjan normaalille toiminnalle ja ohjaa osaltaan palvelujen kehittämistä teknisesti riittävän hyvin skaalautuviksi ja toisaalta sisällöltään laadukkaiksi.

5.4.5. Sosiaalisen median tiedotusmahdollisuudet

2000-luvulla erilaiset käyttäjien tuottaman sisällön jakoon perustuvat verkkopalvelut, niin kutsuttu *sosiaalinen media*, ovat muodostuneet hyvin suosituiksi suomalaistenkin keskuudessa. Palvelut, kuten Facebook ja Twitter, mahdollistavat teksti- ja multimediapäivitysten lähettämisen nopeasti omaa tunnusta seuraavalle käyttäjäjoukolle. Näille palveluille on myös ominaista, että päivitykset voi edelleen jakaa vaivattomasti eteenpäin joko sellaisinaan tai omilla kommenteilla muokattuina omalle seuraajajoukolleen. Täten kiinnostavimpien päivitysten vastaanottajajoukko voi kasvaa lähes eksponentiaalisesti. Sosiaalisen median palvelut ovat myös erinomainen alusta kollektiiviseen tiedonvälitykseen. Hintikan [2010] mukaan kyseessä on ”verkkovoima”: suuri joukko satunnaisesti valikoituneita ihmisiä voi itseorganisoitua projektiksi ja toimia ilman muodollista hierarkiaa tai koordinointia nopeasti, tehokkaasti, tilapäisesti ja globaalisti yhteisen konkreettisen päämärän toteuttamiseksi tietoverkkojen välityksellä (ks. kuva 18).



Kuva 18. Verkkovoiman informaatiotuotannon perusmalli [Hintikka, 2010]

Toisaalta vaarana kansalaislähtöisessä nopeassa verkkoviestinnässä on lähdekritiikin puute ja muut perinteiset ”puskaradion” ongelmat. Varjopuolet konkretisoituivat esimerkiksi Bostonin maratonin pommi-iskujen jälkeen huhtikuussa 2013. Poliisin julkaistua turvakamerakuvia epäillyistä pommittajista alkoi sosiaalisessa mediassa spekulointi epäiltyjen henkilöllisyydestä. Twitter-viesteissä ja Reddit-keskustelufoorumilla levisi nopeasti virheellinen tieto, että epäilty olisi jo aiemmin kadonnut 22-vuotias Brown-yliopiston opiskelija. Starbird ja muut [2013] toteavat, että aiemmissa tutkimuksissa on havaittu joukkoistetun (crowdsourced) informaatiotuotannon korjaavan väärää tietoa (vrt. Hintikan malli). Kuitenkin tutkittuaan Twitter-viestintää Bostonin maratoniskujen jälkeen, he havaitsivat että oikaisut virheellisistä tiedoista peittyivät virheellisen tiedon nopeamman leviämisen alle. Virheellistä tietoa levittävien Twitter-viestien määrä oli kaikissa tutkituissa esimerkkitapauksissa moninkertainen (jopa kymmeniä kertoja suurempi) kuin oikaisuviestien määrä. Virheellisen tiedon levittäminen jatkui myös pidempään kuin korjaukset.

Viranomaiset ovat rantautuneet pikkuhiljaa myös suosituimpiin sosiaalisen mediankin palveluihin. Noin puolella Suomen poliisi- ja pelastuslaitoksista on jo perinteisten WWW-sivujen lisäksi oma sivu Facebook-palvelussa. Pääasiallinen käyttö on kuitenkin toistaiseksi ollut lähinnä yleisluontoista valistusviestintää, uhkaavista onnettomuuksista ei ole tätä kautta vielä tiedotettu. Poliisi on muita viranomaisia paremmin päässyt hyödyntämään sosiaalisen median viestintäkanavia normaalissa toiminnassaan: ”Poliisin tulee olla siellä, missä ihmisetkin ovat. Tekemällä omaa toimintaansa tunnetuksi, tuomalla ihmiskasvot kasvottoman organisaation sijaan esiin ja tarjoamalla uusia kanavia vuoro-

vaikutukseen poliisi haluaa madaltaa kansalaisten kynnystä lähestyä poliisia.” Poliisi mieltääkin sosiaalisen median ennen kaikkea vuorovaikutuskanavaksi, jonka kautta tavoitetaan parhaiten etenkin nuoria. [Poliisi, 2009]

Kuva 19. Tampereen aluepelastuslaitoksen tiedote Facebookissa suuronnettomuusharjoituksesta 25.9.2012.

Tampereen aluepelastuslaitos kokeili syyskuussa 2012 pidetyn suuronnettomuusharjoituksen yhteydessä myös Facebook-tiedottamista harjoituksesta (kuva 19). Pelastuslaitoksen viestintäpäällikkö Veijo Kajánin [2012] mukaan tavoitteena oli selvittää, miten paljon ihmisiä tavoitetaan tätä kautta. Harjoituksesta lähetettiin yhteensä neljä tiedotetta päivän aikana, ja osassa pyydettiin erikseen jakamaan niitä eteenpäin. Facebookin tarjoamien tilastot osoittivat, että tiedotteet tavoittivat parhaimmillaan 41 400 käyttäjää (kun aluepelastuslaitoksen omalla sivulla oli 1078 seuraajaa). On kuitenkin hyvä huomata, että Facebookin logiikka päivitysten näyttämiseen ei ole yksiviivaista, vaan siihen vaikuttavat mm. päivitykseen reagoivien (siitä ”tykkäävien” tai kommentoivien) käyttäjien määrä. Facebook tarjoaa myös mahdollisuuden ostaa päivityksille korkeampaa näkyvyyttä, mutta tätä mahdollisuutta ei Kajánin mukaan käytetty. Facebookin lienee kuitenkin tulevaisuudessa yksi tiedotuskanavista merkittävissä onnettomuuksissa, joskin asiasta toivotaan valtakunnallista linjausta.

Vielä Facebookia helpommin tiedotteiden välittäminen onnistuisi Twitterissä varsin yksinkertaisella toteutuksella, jossa viranomainen (esim. Hätäkeskuslaitos) loisi itselleen varmennetun Twitter-tunnuksen ja välittäisi sen kautta

samat tiedotteet, jotka nykyisellään lähetetään televisiolähetysten ohessa. Tiedotetekstiin voitaisiin liittää ns. *hashtag* sen kunnan nimestä, jonka alueelle tiedote kohdistuu (esim. ”#tampere”), jolloin viestin näkisivät automaattisesti kaikki ”#tampere” hashtagia seuraavat käyttäjät. Twitterin etuna on myös se, että vakiomuotoiset lyhyet viestit voidaan sieltä poimia automaattisesti eteenpäin näytettäväksi esimerkiksi www-sivuille upotettuna tai välittää edelleen eteenpäin toisiin palveluihin.

5.5. Järjestelmän muiden käyttömahdollisuuksien arviointia

CAP-viestiformaatti ja mahdollisuus joustavaan viestinvälitykseen avaavat järjestelmälle myös laajempia käyttömahdollisuuksia kuin pelkän yksisuuntaisen viestinvälityksen. Yksi julkisuudessa esitetty haaste uuden vaaratiedotelain myötä on ollut vaaratiedotteiden käännökset eri kielille. Järjestelmän avulla olisi helppoa välittää luonnosversio viestistä käännösvastuussa olevalle taholle. Esimerkiksi kääntövastuu ruotsiksi välitettävistä viesteistä voitaisiin keskittää Uudenmaan hätäkeskukseen, jolloin mikä tahansa käännöstä vaativa tiedote lähetettäisiin ensin *status = ”Draft”* -muodossa, jonka jälkeen Uudenmaan hätäkeskus lähettäisi siihen päivityksen (*status = ”Actual”, msgType = ”Update”)* sisällyttäen mukaan uuden *info*-elementin, jossa tiedote on käännetty ruotsiksi.

CAP-viestin *info*-elementin rakenteellisia viestiosia (*responseType, headline, description* ja *instruction)* sekä arvioluokituksia *urgency, severity* ja *certaintity* ei ainakaan aluksi käytetä, vaan jotta yhteensopivuus erilaisten jakelujärjestelmien kanssa toimisi, koko viestisisältö on *event*-elementissä. Kuitenkin vastaanottimien kehittyessä (älypuhelimet, Internet-jakelu ym.) tullee mielekkääksi lähettää yhä enemmän tietoa loppukäyttäjille asti. Julkiseksi varoitukseksi tarkoitettu CAP-viesti ei sisällä mitään sellaista tietoa, jota ei voisi sellaisenaan välittää loppukäyttäjille, mutta joidenkin tietojen (esim. *geocode*) osalta viestin rikastaminen ensin jakelujärjestelmässä on mielekästä, jotta päätelaitteet eivät joudu erikseen tätä tekemään.

Viestiväylää voidaan periaatteessa hyödyntää myös muiden kuin CAP-muotoisten viestien välitykseen siihen liitettyjen organisaatioiden välillä. Pitäisin kuitenkin tärkeänä, että vaaratiedotteiden välitys olisi niin loogisesti kuin suurimmalta osalta fyysisestikin oma järjestelmänsä, erillään muista viranomaisten tietojärjestelmistä. Näin vältetään sen ylikuormittuminen tai vikaantuminen sivuvaikutuksena muiden järjestelmien ongelmista. Sen sijaan tietoliikenneyhteyksissä, palvelinkeskustiloissa ja muissa vastaavissa infrastruktuuritoteutuksissa voidaan hyödyntää valtionhallinnon ennestään olemassa olevia keskitettyjä ratkaisuja.

Mikäli vastaavalla arkkitehtuurilla olevia järjestelmiä otetaan käyttöön laajasti myös ulkomailla, ITU-T:n standardoimalla CAP-viestiformaatilla olisi teoriassa mahdollista välittää viestejä yli valtioiden rajojen. Esimerkiksi mahdollisen Yhdysvalloissa tapahtuvan luonnonkatastrofin kohdalla suomalaiset viranomaiset voisivat lähettää IPAWS-järjestelmän kautta ohjetiedotteita vaara-alueella olevien suomalaisten mobiililaitteisiin. Kansainvälisistä kytkennöistä ei kuitenkaan toistaiseksi ole esitetty suunnitelmia missään järjestelmätoteutuksessa.

6. Tietojärjestelmän toteutuksen arviointi

Tietojärjestelmän toteutuksessa on tärkeää huomioida järjestelmän soveltuvuus sille määriteltyjä toiminnallisia ja laadullisia vaatimuksia vasten. Tässä luvussa esittämäni menetelmä on yleiskäyttöinen tietojärjestelmien arkkitehtuurien analysointiin ja arviointiin tarkoitettu ATAM [Kazman *et al.*, 2000]. Menetelmän varsinainen käyttö ja sen pohjana olevat skenaariot tulee määritellä tarkemmin järjestelmän toteutusvaiheessa tilaajien ja toteuttajien keskeKan, mutta pyrin kuvaamaan esimerkinomaisesti, millaisia skenaarioita vasten vaaratiedotteiden välitysjärjestelmää voitaisiin testata.

6.1. Ohjelmistoarkkitehtuurin analysointi ja arviointi

Ohjelmiston arkkitehtuuri edustaa sen varhaisimpia suunnittelupäätöksiä. Sen analysointi kehityskaaren alkuvaiheessa on mielekästä juuri siksi, että mahdolliset ongelmat voivat olla kohtalokkaita ja hankalasti korjattavia myöhemmissä vaiheissa. Koska tämän työn puitteissa ei viedä vaaratiedotejärjestelmän toteutusta korkean tason arkkitehtuuriluonnosta pidemmälle, on mielekästä määrittää juurikin tässä vaiheessa myös analysointimenetelmät. Tällöin arkkitehtuuria voidaan arvioida ja kehittää evolutionaarisena prosessina. Varsinainen arkkitehtuurin analysointi edellyttää useiden tahojen osallistumista (järjestelmän tilaajat ja loppukäyttäjät, kehittäjät ym.), joten itse analyysiprosessin suorittaminen ja sen tulokset jäävät tämän työn ulkopuolella.

Ohjelmistoarkkitehtuuri on käsitteenä vielä melko uusi, ja siten myös arkkitehtuurien analyysimenetelmät alkoivat kehittyä vasta 1990-luvulla. Sen jälkeen arkkitehtuurianalyysiin on kehitetty lukuisia järjestelmällisiä lähestymistapoja, jotka pyrkivät formalisoimaan analysointi- ja arviointiprosessia. Babar ja Gorton [2004] toteavat skenaariopohjaisten menetelmien olevan kypsimpiä ohjelmistoarkkitehtuurin laatuvaatimuksia arvioitaessa. Skenaariotekniikassa esitetään konkreettisia esimerkkitilanteita, joissa valitut laatuvaatimukset tulevat esiin, ja tutkitaan, miten ohjelmiston arkkitehtuuri sopii kyseiseen skenaarioon. He päätyvät pitämään läpikäymistään menetelmistä Carnagie Mellon Universityn kehittämää ATAMia (Architecture Trade-off Analysis Method) käyttökelpoisimpana ja monipuolisimpana valitsemistaan skenaariopohjaisista arviointimenetelmistä. Sen vuoksi olen valinnut sen käytettäväksi tässäkin yhteydessä.

6.2. ATAM-menetelmän vaiheet

ATAM-menetelmässä arvioidaan ohjelmistoarkkitehtuuria laatuvaatimuksia vasten, ja pyritään löytämään mahdollisia arkkitehtuurissa piileviä riskejä. Ni-

mensä mukaisesti ATAM perustuu eri vaihtoehtojen puntarointiin ja tärkeimpien löytämiseen vähemmän tärkeiden kustannuksella. ATAM-menetelmän ei kuitenkaan tarvitse onnistuakseen tuottaa yksityiskohtaista analyysia mistään mitattavasta laatuvaatimuksesta, vaan arvioinnin hyödyt saadaan prosessin läpiviennistä kokonaisuutena.

Kazmanin ja muiden [2000] mukaan muodollinen ATAM-katselmointiprosessi koostuu yhdeksästä vaiheesta, jotka on tarkoitus läpikäydä kahden päivän aikana katselmointitilaisuuksissa, joihin osallistuu riittävä edustus ohjelmiston eri sidosryhmistä (kehittäjistä, ylläpitäjistä, käyttäjistä, tilaajista ym.):

1. ATAMin esittely
2. Liiketoiminnan asettamat vaatimukset
3. Arkkitehtuuriesittely
4. Arkkitehtuurilähestymistapojen tunnistaminen
5. Laatupuun ja skenaarioiden laadinta
6. Arkkitehtuurilähestymistapojen analysointi
7. Skenaarioaivoriihi ja priorisointi
8. Arkkitehtuurilähestymistapojen analysointi
9. Tulosten esittely.

ATAM-skenaario konkretisoi laatuvaatimuksen esimerkillä. Siinä kuvataan vaatimukseen liittyvä tapahtumasarja sekä tasapainopisteet ja riskit. Skenaarion on oltava riittävän täsmällinen, jotta arkkitehtuuria voidaan arvioida sitä vasten. ATAM-prosessin tärkeimmät tulokset ovat keskeisten arkkitehtuuriratkaisujen tunnistaminen, olennaisimpien laatuun vaikuttavien käyttö- ja kehitysskenaarioiden tunnistaminen, laatupuu skenaarioineen (kuvaa laatuvaatimusten ja arkkitehtuuriratkaisujen yhteyden), sekä arkkitehtuuriin liittyvien riskien tunnistaminen.

ATAM-menetelmää kohtaan voidaan esittää kritiikkiä ennen kaikkea skenaarioiden valintaan liittyen. Arviointiin ei välttämättä tule valituksi lopullisen tietojärjestelmän kannalta relevantteja tai edes toteutettuja skenaarioita, tai ne on kuvattu väärällä tavalla. Huonoista skenaariovalinnoista johtuen kaikkia riskejä ei löydetä, eikä menetelmällä ole välttämättä mahdollista edes kaikkia riskejä tunnistaa. Toisaalta ATAM-arviointiprosessin etuna on, että sen oheistuotoksena saadaan arvioitavaan tietojärjestelmään liittyvät tahot tuotua yhteen esittämään monipuolisia näkökulmia, jolloin kaikille osapuolille muodostuu yhtenevä yleiskuva ja saadaan kerättyä arvokasta hiljaista tietoa varhaisessa vaiheessa.

6.3. Vaaratiedottamisen esimerkkitapauksia

Vaaratiedotejärjestelmän toimintaa voidaan peilata arkkitehtuurianalyysissä kuviteltuja, joskin todellisiin tai mahdollisiin tapahtumiin pohjautuvia vaaraskenaarioita vasten. Valitut tapaukset ja niiden käsittely perustuvat Sisäasianministeriön vaaratiedoteoppaan [SM, 2013] esimerkkeihin, vastaavien tapausten uutisointiin mediassa, onnettomuustutkintakeskuksen raportteihin sekä muihin julkaistuihin tutkimuksiin (mm. LVM:n KERTTU-tutkimus vuodelta 2009, josta tarkemmin alakohdassa 6.3.2). Varsinaisessa ATAM-analyysissa tämän kaltaisista tilanteista voidaan johtaa tarkemmat skenaariot valittuja laatuvaatimuksia vasten.

6.3.1. Karhu asutusalueella

Ensimmäisessä skenaariossa on taustatilanteena taajama-alueella havaittu karhu, jonka voidaan olettaa aiheuttavan vaaraa esimerkiksi lenkkeilijöille. Asutusten lähistöllä liikkuvista karhuista on annettu useita hätätiedotteita 2000-luvun aikana, ja ne saavuttivat myös osittain negatiivista julkisuutta valtakunnantason mediassa [HS, 2010], kun hätätiedotteita alettiin välittämään television välityksellä. Ongelmana oli tällöin pienelle alueelle (yksittäinen kunta ja muutamia kaupunginosia, n. 10–30 km halkaisijaltaan oleva alue) tarkoitetun hätätiedotteen leviäminen koko valtakunnan alueelle television välityksellä. Karhuhavainnoista kertovien uutisten pohjalta olen luonut kuvitteellisen tyypillisen tilanteen, joka on kuvattu taulukossa 5.

Alkutilanne	Hätäkeskus on saanut ilmoituksen karhuhavainnosta. Havaintopaikan ja pedon käyttäytymisen perusteella päätetään, että eläin voi kohdattaessa aiheuttaa vaaraa alueella oleville. Hätäkeskus määrittää vaikutusalueen ja lähettää hätätiedotteen, sekä käynnistää poliisin johtaman petoeläimen etsinnän.
Maantieteellinen vaikutusalue	Muutama kaupunginosa tai 1-3 kuntaa. Maantieteellisesti 10–30 km halkaisijaltaan oleva alue. Rajaus perustuu karhusta saatuihin havaintoihin. Uusien havaintojen myötä vaikutusalue voi siirtyä pedon kulkusuunnan mukaan.
Välittömässä vaarassa olevat	Karhun metsäisellä ulkoilualueella, esimerkiksi lenkkipolulla arvaamatta kohtaavat. Ulkona leikkivät lapset. Käytännössä vaarassa olevien määrän voidaan arvella olevan samaa luokkaa pedon nähneiden ja siitä hätäkeskukseen ilmoittaneiden kanssa, eli n. 5-20 henkeä.
Vaaditut toimenpiteet	Ihmisiä kehotetaan poistumaan alueelta ja siellä asuvia pysymään sisätiloissa.
Tilanteen kesto	Joitakin tunteja – 1 vuorokausi.
Tilanteen kehitys	Uusien havaintojen myötä viranomaiset tiedottavat vaikutusalueen

	muutoksista. Kun pedon havaitaan poistuneen asutuksen lähistöltä, siitä ei ole enää saatu havaintoja tai uhka on muuten poistunut viranomaiset tiedottavat asiasta tiedotusvälineiden kautta.

Taulukko 5. Skenaarion "Karhu asutusalueella kuvaus".

Tässä skenaariossa konkreettisen henkeä tai terveyttä uhkaavan vaaran riski on melko pieni suhteessa kohdealueella oleviin ihmisiin. Kuitenkin, koska eläimen tarkkaa sijaintia tai käyttäytymistä ei tiedetä, on perusteltua varoittaa kaikkia alueella olevia. Lisäksi vaaratiedotteen myötä ihmiset valpastuvat ja ilmoittavat tarkemmin eläimen uusista liikkeistä hätäkeskukseen, jolloin tilannekuva tarkentuu ja vaikutusaluetta voidaan kohdistaa paremmin. Analogia tälle skenaariolle on uhkaavasti käyttäytyvän aseistetun henkilön liikkuminen tietyllä alueella.

6.3.2. Vaarallisen aineen onnettomuus

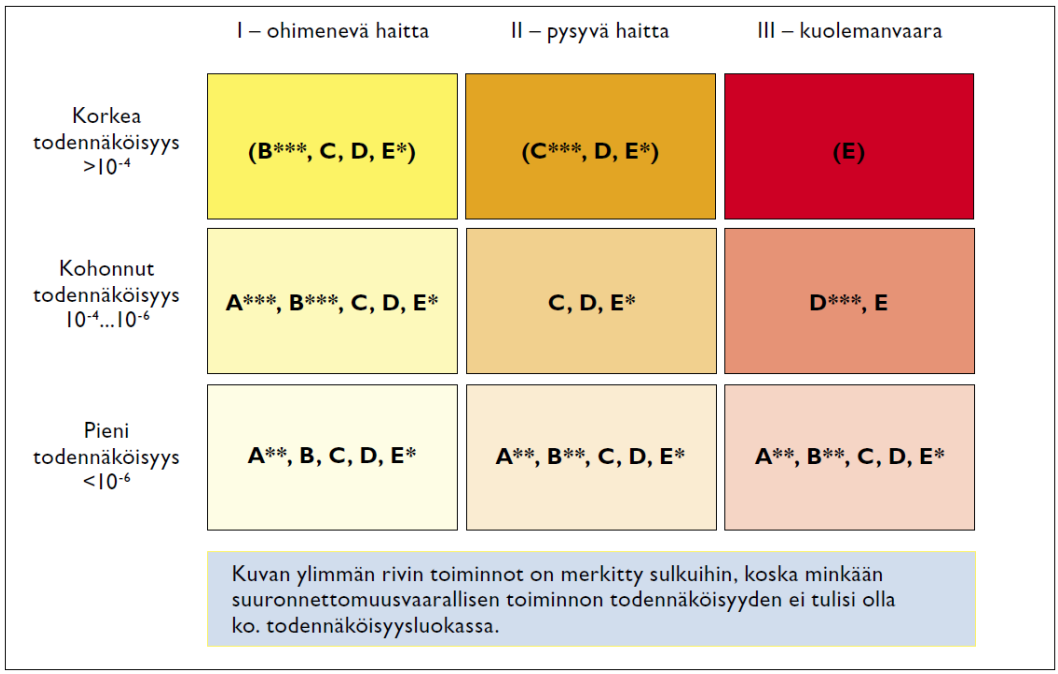
Perinteisesti suuronnettomuudeksi miellettyjä onnettomuuksia ovat erilaiset vaarallisiin aineisiin, kuten kemikaaleihin liittyvät onnettomuudet. Näitä voivat olla esimerkiksi vuodot säiliöissä teollisuuslaitoksilla, ratapihoilla tai maantiekuljetuksissa. Myös tulipalot tai räjähdykset teollisuuslaitoksissa saattavat vapauttaa vaarallisia aineita, joiden vaikutusalue voi ulottua useiden kilometrien päähän tuuliolosuhteista riippuen. Vaikka vaarallisten aineiden kuljetuksiin (VAK) käytetyt ratapihat sekä teollisuusalueet yleensä sijoitetaankin etäämmällä asutuksesta, saattaa onnettomuuden vaikutusalueella silti olla tuhansia ihmisiä, vakituisten asukkaiden lisäksi esimerkiksi muiden teollisuusalueella sijaitsevien rakennusten työntekijöitä.

VAK-liikenteen riskejä on tarkasteltu LVM:n koordinoimassa KERTTU-hankkeessa, jonka tavoitteina oli mm. tunnistaa ja arvioida mahdollisia riskienhallintakeinoja liikenteen solmukohtien suuronnettomuusriskin vähentämiseen. Hankkeen tulokset ovat myös sovellettavissa esimerkiksi rajanylityspaikkojen, tieliittymien ja risteysten sekä tietyin rajauksin tunneleiden riskiarviointitulosten esittämiseen [LVM, 2009]. KERTTU-hankkeen tuloksena on luotu luokitteluehdotus eri riskitason alueille (taulukko 6) ja sen pohjalta kuvassa 20 esitetty riskitason hyväksyttävyys eri toimintojen sijoittamiselle.

Luokka	Sallitut toiminnot
A	Tiheään rakennetut asuinalueet, sairaalat, koulut, vanhainkodit, päiväkodit, kauppakeskukset, yleisötilaisuudet
B	Harvemmin rakennetut asuinalueet, julkiset palvelut, yliopistot, rautatieasemat ja vastaavat keskittymät
C	Harvaan asutut alueet, toimistot, loma-asutus, kohteet, joissa epäsäännölli-

	nen ihmisvirta (virkistysalueet, hautausmaat), logistiikka
D	Haja-asutusta, maataloutta, teollista tuotantoa
E	Teollista tuotantoa, jossa ei asiakasvirtoja, VAK-keskittymät
Lisämerkinnät: * = toiminnot eivät saa tuoda uusia riskejä ** = toiminnot voidaan sallia, mikäli saavutettavat yhdyskuntarakenteen muut hyödyt ovat riittävän suuret (uudisrakentaminen) tai alueella on muita vastaavia riskejä, esimerkiksi liikennettä *** = edellisen lisäksi tiedotettava riskille altistujille säännöllisesti sekä huomioitava kaikissa pelastussuunnitelmissa.	

Taulukko 6. Toimintojen luokittelu

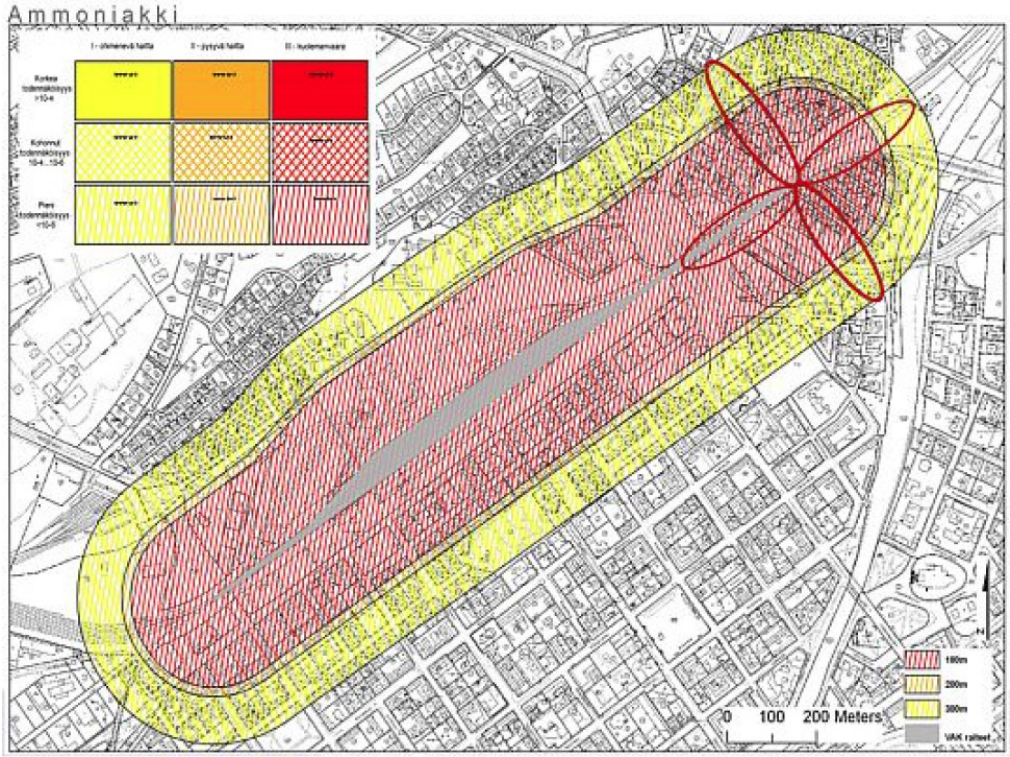


Kuva 20. Riskitason hyväksyttävyys eri toimintojen sijoittamiselle

KERTTU-hankkeessa luodut menetelmät mahdollistavat myös suuronnettomuuksien vaikutusalueen havainnollistamisen esittämällä riskit karttapohjalla ja käyttäen sovittua värikoodausta vaikutusalueilla.

Olen ottanut suoraan KERTTU-raportissa esimerkkinä käytetyn skenaarion, jossa Turun ratapihalla tapahtuu ammoniakkivuoto. Onnettomuuden vaikutusalueeksi on määritelty ohimenevän haitan osalta 300 metriä, pysyvän haitan osalta 200 metriä ja kuolemanvaaran osalta 180 metriä. Kuvassa 21 on havainnollistettu kuvitteellisen ammoniakkivuodon vaikutusalueet. Ammoniakki leviää kapeana pilvenä tuulen alapuolelle. Yksittäisen vuoden vaikutusalue on havainnollistettu punaisena soikiona ja yhteensä kaikki mahdolliset vuotopaikat muodostavat ratapihaa ympäröivän vaikutusalueen [LVM, 2009]. KERTTU-hankkeen loppuseminaarissa pidetyn esityksen materiaaleista käy ilmi, että 1

km säteellä ratapihasta on n. 22 000 asukasta, lisäksi kouluja, päiväkoteja, sairaaloita, kauppoja sekä kokoontumistiloja [Hovi, 2009].



Kuva 21. Kuvitteellisen Turun ratapihalla sattuneen ammoniakkivuodon vaikutusalue

Alkutilanne	Hätäkeskus on saanut ilmoituksen vaarallisen aineen vuodosta. Aineen ominaisuuksien ja vallitsevien tuuliolosuhteiden johdosta pelastuslaitos antaa vaaratiedotteen.
Maantieteellinen vaikutusalue	Maantieteellisesti 2-10 km halkaisijaltaan oleva alue. Vallitsevat tuulet vaikuttavat merkittävästi alueen määrittelyyn ja tarvittaessa aluetta voidaan laajentaa.
Välittömässä vaarassa olevat	Tuulen alapuolella lähellä vuotopaikkaa ulkotiloissa olevat.
Vaaditut toimenpiteet	Lähimpänä olevia kehotetaan poistumaan alueelta. Kauempana olevia kehotetaan pysymään sisätiloissa ikkunat ja ilmanvaihto sulkien sekä seuraamaan viranomaisten tiedottamista tilanteen kehityksestä.
Tilanteen kesto	Joitakin tunteja – 1 vuorokausi.
Tilanteen kehitys	Kun vuoto on saatu tukittua, vaarallisen aineen muodostama kaasupilvi hajoaa muutamien tuntien kuluessa. Alkuperäisen tiedotteen jakelulla lähetetään ”vaara ohi” –tiedote sekä tiedotetaan asiasta joukkoviestimien välityksellä.

Taulukko 7. Skenaarion ”Vaarallisen aineen onnettomuus” kuvaus

6.3.3. Vaarallisen voimakas myrskytuuli

Suomea uhkaavista varsinaisista luonnononnettomuuksista todennäköisimpiä ovat vaaralliset myrskytuulet, jotka aiheuttavat laaja-alaisia tuhoja mm. kaatuneiden puiden ja irronneiden rakennusten katteiden osalta. Myrskyjen seurauksena myös yhteiskunnan normaalit toiminnot voivat häiriintyä etenkin sähkönjakelun ja tietoliikenteen osalta. Myrskyt saattavat edetä nopeasti laajoille maantieteellisille alueille. Nykyisen vaaratiedotelain mukaan Ilmatieteen laitos voi omatoimisesti antaa vaaratiedotteen, kun yllättävä voimakas sääilmiö uhkaa.

Myrskytuulen suurin riski kohdistuu vesi- ja ilmailuliikenteeseen. Näiden kaupallisilla toimijoilla on yleensä jo ennestään käytössään vakiintuneet tavat säätiedotteiden seuraamiseen ja poikkeuksellisten sääolosuhteiden aiheuttama riski vaihtelee aluksen ja reitin mukaan. Sen sijaan tavalliset kansalaiset eivät yleensä ole varautuneet vaaralliseksi yltyviin ukkosmyrskyihin, joissa riskinä ovat mm. kaatuvat puut. Varsinaisen myrskyn jälkeen ongelmia saattavat aiheuttaa myös pitkään poikki olevat sähkö-, viestintä- ja liikenneyhteydet.

Alkutilanne	Ilmatieteen laitos ennustaa lähitunteina voimakkaita ukkoskuuroja, joiden yhteydessä tuulen nopeus puuskissa voi nousta yli 15 metriin sekunnissa.
Maantieteellinen vaikutusalue	Yksi tai useampia maakuntia.
Välittömässä vaarassa olevat	Tuulen äkillisesti irrottamien esineiden (kattopellit, kaatuvat puut ym.) tiellä olevat. Tilanteen pitkittyessä sähkönjakelun häiriöt voivat myös aiheuttaa vaaratilanteita.
Vaaditut toimenpiteet	Ihmisiä kehotetaan pysymään sisätiloissa. Tilanteen pitkittyessä ohjeistetaan varautumiseen.
Tilanteen kesto	Puolesta vuorokaudesta pariin vuorokauteen.
Tilanteen kehitys	Uusien havaintojen myötä viranomaiset tiedottavat vaikutusalueen muutoksista.

Taulukko 8. Skenaarion "vaarallisen voimakas myrskytuuli" kuvaus

Taulukossa 8 on listattu myrskytuuleen liittyvän vaaratiedottamisen ominaisuuksia. Myrsky eroaa muista vaaratilanteista siinä mielessä, että mahdollinen vaikutusalue on melko laaja, mutta on vaikeaa yksilöidä tiettyjä kohteita, joissa hengenvaara on todellinen.

6.3.4. Ulkomailla sattunut luonnononnettomuus

Ulkomailla on suurempi riski laaja-alaisempaa tuhoa aiheuttaville luonnononnettomuuksille kuin Suomessa. Maanjäristysten ja niitä seuraavien tsunamien

lisäksi myös tulvat, tornadot ja maastopalot voivat aiheuttaa suuronnettomuustilanteita laajalle alueelle. Mikäli onnettomuusalueella on paljon suomalaisia matkailijoita, on perusteltua varoittaa heitä onnettomuudesta ja tiedottaa evakuoinneista takaisin kotimaahan myös Suomen viranomaisten toimesta. Varoitusjärjestelmien kehittyessä paikalliset viranomaiset saattavat kyetä hoitamaan varsinaisesta vaaratilanteesta varoituksen ennakkoon, jolloin suomen viranomaisten tärkeimmäksi tehtäväksi jää kansalaisten tavoittaminen ja evakuointilennoista tiedottaminen.

Alkutilanne	Ulkomailla on sattunut laaja-alainen luonnonkatastrofi, esim. maanjäristys. Kohdealueella tiedetään olevan runsaasti suomalaisia matkailijoita.
Maantieteellinen vaikutusalue	Vaaratiedotejärjestelmän näkökulmasta yksi kokonainen valtio. Tiedotteiden sisällössä voidaan kertoa tarkemmin vaikutusalueesta.
Välittömässä vaarassa olevat	Katastrofin vaikutusalueella kohdemaassa olevat. Luonnonkatastrofit voivat aiheuttaa laajoja häiriöitä maan infrastruktuuriin, kuten viestiyhteyksiin, liikenteeseen ja sairaanhoitoon.
Vaaditut toimenpiteet	Ihmisiä kehotetaan seuraamaan paikallisten viranomaisten ohjeita ja ohjeistetaan yhteydenottotavoista Suomen edustustoon.
Tilanteen kesto	Parista vuorokaudesta useisiin viikkoihin.
Tilanteen kehitys	Mikäli erillisiä evakuointilentoja järjestetään, niistä tiedotetaan uusilla tiedotteilla maassa olevia.

Taulukko 9. Skenaarion "Ulkomailla sattunut luonnononnettomuus" kuvaus

Ulkomailla sattuneessa onnettomuudessa korostuu tarve kaksisuuntaiseen viestintään, sillä alueella olleiden omaiset haluavat saada tiedon siitä, ovatko matkalaiset kunnossa. Toisaalta myös viranomaisilla voi olla tarvetta selvittää nopeasti evakuoinnin tarpeessa olevien lukumäärä ja yhteystiedot. Joissakin ulkomaisissa hankkeissa ja tutkimuksissa on esitetty olennaisena osana vaaratiedotejärjestelmään myös kuittausmahdollisuutta viestin vastaanoton jälkeen, mutta nähdäkseni tarve tällaiselle on sen verran tapauskohtainen ja järjestelmän toteutusta monimutkaistava, että se voidaan toteuttaa erillisenä. Tällöin vaaratiedotteessa voidaan ilmoittaa mukana toimintaohjeet esim. kuittaustekstiviestin lähettämisestä, jolla vastaanottaja voi ilmoittaa tilanteensa.

7. Yhteenvetoa

"Vaaratiedote pitäis myös antaa siitä jos joku ajaa autolla liian lähellä puskuria tai jos kaupat on kiinni sunnuntaisin."

Nimimerkki "Turha holhoaminen" uutiskommenteissa [YLE, 2013]

7.1. Vastaukset tutkimuskysymyksiin

Alkuperäinen motivaationi aihevalinnan taustalla oli selvittää, ovatko matkapuhelimiin välitettävien vaaratiedotteiden toteutuksen viivästymisen syynä tekniset haasteet. Aihe laajeni kuitenkin pian kattamaan monikanavaisen vaaratiedotteiden välitysjärjestelmän määrittelyn, sillä pelkkä yhden jakelukanavan tekninen toteutus ei ole kokonaisuuden kannalta merkittävä ongelma. Suomalaisessa julkisessa keskustelussa ja lainsäädännön valmistelussa vaikutetaan kuitenkin jämähtäneen liikaa pieniin yksityiskohtiin, kuten tiedotteiden kaksikielisyyden tai vaaratiedotetekstiviestin kulujen korvaamiseen. Vaaratiedottamisen ydin, eli välittömässä vaarassa olevien kansalaisten mahdollisimman tehokas tavoittaminen, tuntuu jääneen taustalle. Olennaista ei ole, miten vaarassa oleva saa varoituksen, vaan se, että varoitus yleensä saadaan.

Kattava vaaratiedottaminen vaatii keskitetyn viestien välitysjärjestelmän, jonka kautta toimivaltaiset viranomaiset voivat helposti lähettää vaaratiedotteita erilaisten jakelukanavien kautta. Tällaista ei ole tietääkseni aiemmin suunniteltu Suomessa, mutta kansainvälisten hankkeiden, kuten EU-Alertin, CMAS/WEA:n ja 3GPP:n määritysten mukainen yleisarkkitehtuuri soveltuu nähdäkseni hyvin myös suomalaisiin tarpeisiin. Järjestelmän ydin on yksinkertainen viestiväylä, jonka ylitse välitetään vakiomuotoisia vaaratiedoteviestejä. Viestimuodoksi on jo olemassa valmis rakenteinen CAP-formaatti, jota on helppo soveltaa Suomen tarpeisiin. Vakioitu ja avoin viestiformaatti mahdollistaa myös julkiselle tietojärjestelmälle olennaiset avoimet rajapinnat, jolloin järjestelmään liittyviä muita tietojärjestelmäkomponentteja (joko vaaratiedotteita syöttäviä tai niitä välittäviä) voivat toteuttaa ja tarjota lukuisat eri toimittajat ilman erillisiä kuluja.

Keskitetty vaaratiedotteiden välitysjärjestelmä ei ole edellytys nykyisten TV- ja matkapuhelinvaaratiedotteiden parantamiselle, vaan se voidaan toteuttaa erillisenä hankkeena näistä riippumatta. Toisaalta esittämäni kaltainen järjestelmä mahdollistaa lukuiset uudet tiedotteiden välitysjärjestelmät (viranomaisten verkkopalvelut, sosiaalinen media, automaattiset integroinnit joukkoviestimiin), joiden myötä vaaratiedotteiden tavoittavuus todennäköisesti paranee huomattavasti. TV:n vaaratiedotteiden rajaaminen nykyistä pienemmälle alueelle vähentää epärelevanteista tiedotteista aiheutuvaa ärsytystä, ja tuki-

asematarkkuudella lähetettävät CBS-tiedotteet tavoittavat nopeasti kohdealueella olevat, mutta mikään järjestelmä ei yksinään ole riittävä. Jotta vaaratiedottamisen perimmäinen tarkoitus toteutuisi, viestin perillemenon todennäköisyyttä tulee kasvattaa lukuisilla rinnakkaisilla järjestelmillä. Keskitetty vaaratiedotteiden välitysjärjestelmä mahdollistaa tämän helposti.

7.2. Kohdennetun vaaratiedotejärjestelmän toteutuksen tilanne

Tutkimukseni lähti liikkeelle kohdennetuista vaaratiedotteista, eli käytännössä matkapuhelimiin toimitettavista viesteistä. Sisäasiainministeriön asettama viranomaistiedotteiden antamista selvittänyt työryhmä ehdotti loppuraportissaan [SM, 2010a], että:

1. Viranomaisten toimivallasta ja vastuusta antaa viranomaistiedotteita tulisi säätää lailla.
2. Viranomaistiedotteiden antamisesta ja kääntämisestä tulisi antaa yleisohje sisäasiainhallinnon viranomaisille.
3. Viranomaistiedotteiden käännättämisestä huolehtiminen (ruotsiksi suomeksi, saamelaisten kotiseutualueella saameksi ja tilanteen niin edellyttäessä myös muille vieraille kielille) tulisi olla Hätäkeskuslaitoksella.
4. Hätätiedotteet tulisi voida antaa myös alueellisesti.
5. Kohdennetun viranomaistiedotteen käyttöä nykyistä varoitusjärjestelmää täydentävänä teknologiana tulisi kehittää.
6. Uutta viestintäteknologiaa tulisi hyödyntää nykyistä suunnitelmallisemmin kansalaisten varoittamisessa.

Nämä suositukset annettiin elokuussa 2010. Neljässä vuodessa suosituksista on toteutettu käytännössä vain kohdat 1-3. Sen sijaan loppujen osalta on toistaiseksi näkynyt vain vähän konkreettisia toimia.

Kansallisten infrastruktuurihankkeiden toteutus on kiinni aina poliittisista päätöksistä ja tahdosta niiden eteenpäin viemiseksi. Kansalliseen turvallisuuteen liittyviä järjestelmiä kehitetään harvoin proaktiivisesti, vaan sysäyksenä niille on useimmiten jokin kriisi, jonka jälkipuinnissa peräänkuulutetaan uusia menetelmiä ja parannuksia viranomaistoimintaan. Tämä kehitys on nähtävissä ulkomaillakin: Japanissa jatkuvat luonnonkatastrofit ovat pakottaneet kehittämään sofistikoituneet järjestelmät, Yhdysvalloissa puolestaan hurrikaani Katrina ja terrorismiuhka toimivat alkuunpanijoina. Meillä on kuitenkin nähtävissä kolme selkeää omaa ongelmaa poliittisessa päätöksenteossa ja sitä valmistelevassa virkamiestyössä, mitkä vaikuttavat hidastavan vaaratiedotejärjestelmien kehitystä:

1. ”Kaikki tai ei mitään” -asenne. Yksittäiseltä järjestelmältä odotetaan kaiken kattavaa toimintaa, muussa tapauksessa sitä ei toteuteta lainkaan (esimerkkinä perustelut SMS-vaaratiedotteille CBS:n sijaan). Kuitenkin todellisuudessa mikään järjestelmä ei tavoita kaikkia, vaan kattavuus paranee ainoastaan usealla rinnakkaisilla, toisiaan täydentävällä järjestelmällä.
2. Vastuunkantajan ja rahoittajien pallottelu. Vaaratiedotejärjestelmän maksajaa ja vastuutahoa on haettu niin liikenne- ja viestintäministeriön alta kuin sisäasiainministeriönkin toimialalta sekä työ- ja elinkeinoministeriön alaisesta Huoltovarmuuskeskuksesta (toisaalta taas valtion yleiset tietojärjestelmät kuuluvat valtiovarainministeriön alaisuuteen). Absurdina lisäpiirteenä on huoli teleoperaattoreiden laskutuksesta varoitusten välittämisestä (mille ei ole konkreettisia perusteita ainakaan kotimaassa), kun tämä voitaisiin säätää lailla ilman korvausta tehtäväksi.
3. Yksityiskohtiin takertuminen. Edellisessä lainsäädännön uudistusprosessissa keskeiseen osaan nousi koko vaaratiedottamisprosessin kannalta melko triviaali kielikysymys ruotsinkielisistä hätätiedotteista. Sen sijaan vaaratiedotelain ulkopuolelle jätettiin kokonaan jakelupuoli eli varsinainen vaarassa olevien tavoittaminen.

Suomen kannalta lohdullisena näenkin, että kansainvälinen kehitys näyttää tuovan ulkomailla toimivaksi havaittuja ratkaisuja yleisiksi standardeiksi vakioituina valmiiksi matkaviestinverkkoihin sekä mobiilipäätelaitteisiin. Kenties tätä myötä Suomessakin avautuu mahdollisuus järjestelmän toteuttamiselle aiempaa helpommin, kun tekniset valmiudet verkoissa ja päätelaitteissa kasvavat vaivihkaa.

7.3. Matkaviestinverkkojen ja Internet-palvelujen kehitys

Laitevalmistajat ja operaattorit ovat innokkaita tuomaan globaalien matkaviestinverkkojen uusia ominaisuuksia mahdollisimman nopeasti kuluttajien saataville uusien liiketoimintamahdollisuuksien toteuttamiseksi. Ominaisuudet on kuitenkin standardoitava 3GPP:n kaltaisten yhteistyötahojen avulla, jotta päätelaitteet sekä verkon komponentit toimisivat saumattomasti yhteen eri maissa ja eri operaattoreilla laitevalmistajista riippumatta. Esimerkiksi alkuperäinen tekstiviestivälitys on ollut mukana jo varhaisimmasta 3GPP:n määrityksistä alkaen, kun taas sijaintipohjaiset palvelut (LCS) ovat muuttuneet vähitellen kypsemmiksi vuosien varrella julkaistuissa päivitysversioissa. Uudet tekniikat niin radioverkoissa (UMTS, LTE) kuin runkoverkonkin puolella vaikuttavat osaltaan standardien kehitykseen. Tämä näkyy toisaalta abstraktiotason lisääntymisenä ja teknologia-agnostisempina verkkoelementteinä ja toisaalta toiminnallisuu-

den pilkkomisena pienempiin osakomponentteihin ja uusien rajapintojen määrittelyssä niiden välille.

Toisaalta se, että jokin ominaisuus on määritelty 3GPP:n ja ETSIn tai vastaavien standardeihin ja verkon pitäisi se nimellisesti toteuttaa, ei vielä takaa että toiminto olisi aidosti käyttökelpoinen. Esimerkiksi tilaajien paikannus LCS-määrityksen pohjalta toimii yksittäisiin liittymiin, mutta odottamattomiin vaaratilanteisiin varautuminen koko maan laajuisesti vaatisi jatkuvaa sijaintitiedon keräämistä miljoonista liittymistä, mihin verkot eivät vielä skaalaudu. Sama ongelma on vaaratiedotteen lähettämisessä suurelle kohdejoukolle massatekstiviesteillä. Uusien toimintojen saaminen käyttökuntoon vaatii yleensä operaattoreilta investointeja verkkojen päivittämiseksi, ja toisaalta laitevalmistajatkaan eivät aina tuo heti kaikkia toimintoja mukaan laitteisiinsa.

Vajaassa kymmenessä vuodessa Aasian tsunamikatastrofin jälkeen tyypilliset suomalaisten päätelaitteet ovat kuitenkin muuttuneet merkittävästi. Vuonna 2004 valtaosa puhelimista oli Internet-ominaisuuksiltaan vielä varsin rajallisia, eikä niissä ollut sisäänrakennettua GPS-vastaanotinta. Nykypäivänä lähes kaikki uudet puhelimet ovat täysiverisiä älypuhelimia, joista löytyy vakiona nopeat pakettidatayhteydet sekä GPS- ja verkkopaikannus. Puhelimen toiminnallisuuden laajentaminen onnistuu peruskäyttäjiltäkin helposti sovelluskauppojen avulla, joissa on saatavilla valtava määrä uusia kolmansien osapuolten sovelluksia, myös vaaratiedoteviestintään tarkoitettuja [Hokkanen *et al.*, 2013]. Suurien kosketusnäyttöjen myötä älypuhelimet ohittavat jo pöytäkoneet yleisimpänä väylänä Internetin käytölle. Vastaavasti sosiaalinen media on muuttanut Internetin käyttöä merkittävästi yhä enemmän matalan kynnyksen kaksisuuntaiseen viestintään, kun se vielä 2004 oli enemmän muodollista yksisuuntaista tiedon selaamista.

7.4. Loppusanat

Varautuminen poikkeustilanteisiin on aina haasteellista, sillä siihen liittyvien asioiden merkitystä ei välttämättä havaita riittävästi normaaliolosuhteissa. Julkisen talouden jatkuvissa säästöohjelmissa pyritään keskittymään lyhyellä aikavälillä saavutettaviin etuihin, eikä harvinaisiksi miellettäviä poikkeustilanteita nähdä kovin merkityksellisenä asiana.

Toisaalta kuitenkin tieto- ja viestintätekniikan kehityksen myötä samoja järjestelmiä voitaisiin käyttää huomattavasti matalammalla kynnyksellä ja paljon tehokkaammin kuin perinteisiä väestöhälytysmenetelmiä. Kansalaiset omaksuvat yllättävänkin nopeasti uudet teknologiat, siitäkin huolimatta että niitä tuntuu tulevan ja menevän jatkuvasti kiihtyvällä tahdilla. Mikäli viranomaiset ha-

luavat säilyttää uskottavuutensa ja tavoittaa kansalaiset tehokkaimmilla tavoilla, tulee niiden myös pysyä mukana teknisessä kehityksessä.

Vaaratiedotejärjestelmän kotimaisen toteutuksen pitkä tie kuvastaa hyvin suomalaisen yhteiskunnan asenteita ja muutoksia 2000-luvulla. Normaalitilanteessa järjestelmille ei tunnu löytyvän maksajaa, mutta poikkeustilanteiden sattuessa varoitusjärjestelmän puuttumista ihmetellään ja vastuuta peräänkuulutetaan. Lainsäädännön uudistuksissa suurin huomio keskittyy kaksikielisyyden vaalimiseen, ei siihen, että vaaratiedotteita saataisiin paremmin perille. Teknisesti haastavamman SMS-teknologian valinta CBS-teknologian sijaan vaaratiedotetekstiviestien toteutustavaksi vuonna 2005 kuvastaa aikansa syvää luottamusta kotimaiseen viestintäteknologian osaamiseen. Tästä huolimatta nyt, lähes kymmenen vuotta myöhemmin, yhtäkään alueellisesti kohdistettua tekstiviestivaaratiedotetta ei ole lähetetty. Mobiiliteknologian kehittymisen myötä kännykät ovat muuttuneet monipuolisiksi Internet-päätelaitteiksi ja verkkoihinkin on tullut runsaasti ominaisuuksia. Nokian merkityksen vähentyessä kenties Suomessakin huomataan, että vastaavia ja parempia järjestelmiä toteutetaan jo hyvää vauhtia muuallakin, ja niitä voitaisiin ottaa yllättävän helposti käyttöön täälläkin.

Pelastusopiston ja Poliisiammattikorkeakoulun viime vuoden aikana tehty tutkimushanke *Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa* [SM, 2014] käsitteli pitkälti samoja aiheita kuin oma tutkimukseni. Vaikka en ollutkaan hankkeesta tietoinen omaa työtäni kirjoittaessa, havaitsin ilokseni, että myös tässä tutkimuksessa on päädytty moniin samoihin johtopäätöksiin kuin omassanikin. Jälkimmäisessä väliraportissa esitellään WEA-järjestelmä ja CAP-tietomalli esimerkkinä ulkomaisesta kehityksestä, ja loppuraportti päätyykiin ehdottamaan cell broadcast -teknologiaan pohjautuva järjestelmiä. Samoin korostetaan monikanavaisen hätäviestinnän etuja, johon sosiaalisen median palvelut istuvat luontevasti. Hankkeessa käytiin läpi myös runsaasti kaksisuuntaista viestintää, eli miten kansalaisilta erilaisten uusien viestintäteknologioiden avulla saatava tieto puolestaan auttaisi viranomaisia hätätilanteissa.

Turvallisuusalan viranomaisten itse tekemä tutkimus todennäköisesti saa laajempaa huomiota alalla, ja kannustaa viranomaisia kehittämään toimintaansa siinä esitettyjen ehdotusten mukaisesti. Toivonkin Suomen viranomaisille uskallusta kokeilla rohkeasti uusiakin teknologioita, ja halua pyrkiä eroon ”kaikki tai ei mitään” -ajattelusta. Päättäjiltä puolestaan toivon kaukonäköisyyttä turvata resurssit sellaisillekin palveluille, jotka eivät välttämättä pääse osoittamaan todellista arvoaan vielä heidän vaalikautensa aikana.

Viiteluettelo

[3GPP, 2011] *3GPP Releases*. Saatavilla: *http://www.3gpp.org/Releases.*

[3GPP TS 22.268, 2011] *3GPP TS 22.268 V11.3.0, Public Warning System (PWS) requirements (Release 11).* 3GPP, 2011.

[Aamulehti, 2011] Missä on Karoliina Kestin matkapuhelin? Aamulehti 9.9.2011. Saatavilla: *http://www.aamulehti.fi/Kotimaa/1194695955783/artikkeli/missa+on+karoliina+kestin+matkapuhelin+.html* [Viitattu 7.4.2012].

[Ahonen, 2008] Paavo Ahonen, *Funet - Suomen tie internetiin*. CSC – Tieteen tietotekniikan keskus Oy, Helsinki, 2008.

[Aloudat & Michael, 2011] Anas Aloudat and Katina Michael, The application of Location Based Services in National Emergency Warning Systems: SMS, Cell Broadcast Services and Beyond" *In: Proceedings of the National Security Science and Innovation Conference*. Canberra: Research Network for a Secure Australia, 2011. Available at: *http://works.bepress.com/kmichael/218/.*

[Aloudat *et al.* 2007] A. Aloudat, K. Michael and J. Yan, Location-Based Services in Emergency Management – from Government to Citizens: Global Case Studies. In: Mendis, P, Lai, J, Dawson, E and Abbass, H, *Recent Advances in Security Technology*. Australian Homeland Security Research Centre, Melbourne, 2007, 190-201.

[Barnett, 2011] Alexander G. Barnett, A Study of Social Media Integration in Public Emergency Alert Systems. Master's Thesis, Purdue University, 2011. Available at: *http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1038&context=techmasters.*

[CHORIST, 2008] CHORIST SP3.D55 Deliverable. Lessons learned by Delft University of Technology on Emergency Warnings. TU Delft, Delft, 2008. Available at: *http://www.chorist.eu/doc/CHORIST-SP3.D55-V1.1.pdf.*

[ETSI, 2000] ETSI TS 100 522 v7.1.0. Digital cellular telecommunications system (Phase 2+); Network architecture. ETSI, 2000.

[ETSI, 2012] ETSI TS 102 900 v1.2.1. Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service. ETSI, 2012.

[ETSI, 2013a] ETSI TS 123 271 v11.2.0. Digital cellular telecommunications system (Phase 2+); Functional stage 2 description of Location Services (LCS). ETSI, 2013.

[ETSI, 2013b] ETSI TS 123 040 v11.5.0. Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS). ETSI, 2013.

[FCC, 2013] Legal and Regulatory Framework for Next Generation 911 Services, Federal Communications Commission, 2013. Available at: *http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-319165A1.pdf.*

[FEMA, 2010] Strategic Plan for the Integrated Public Alert System (IPAWS) Program, US Federal Emergency Management Agency (FEMA), 2010. Available at: *http://www.fema.gov/pdf/emergency/ipaws/ipaws_strategic_plan.pdf.*

[FEMA, 2013] Wireless Emergency Alert issued by Massachusetts Emergency Managment Office ordering Shelter In Place during the Bosting Marathon Bombing, US Federal Emergency Management Agency (FEMA), 2013. Available at: *http://www.fema.gov/media-library/assets/images/34741*

[Ficek *et al.*, 2010] Michal Ficek, Tomás Pop, Petr Vlácil and Katerina Dufkova, Performance Study of Active Tracking in a Cellular Network Using a Modular Signaling Platform. Available at: *http://www.rdc.cz/download/publications/p239-ficek.pdf*.

[Google, 2012] The Official Google.org Blog: Public Alerts now on Google Maps, Google, 2012. Available at: *http://blog.google.org/2012/01/public-alerts-now-on-google-maps.html.*

[Guardian, 2014] Text message warn Ukraine protesters they are "participants in mass riot". The Guardian, 21.1.2014. Available at: *http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot.*

[Harju, 2009] Jukka Harju, Tv:n hätätiedotteita ei vielä saada alueellisiksi. Helsingin Sanomat, 12.7.2009.

[Hietalahti *et al.*, 2010] Hannu Hietalahti, Kevin Holley, Stephen Hayes and Brian Daly, *PWS Public Warning System*. Presentation in IETF #79 Conference, 2010. Saatavilla: *http://www6.ietf.org/proceedings/79/slides/atoca-0/atoca-0.htm*

[Hintikka, 2010] Kari A. Hintikka, Verkkovoima uutistuotannon muotona – sikainfluenssa ja Iranin levottomuudet internetissä. Teoksessa *Journalismikritiikin vuosikirja 2010*, Katariina Kyrölä (toim.), Tampere, 2010, 100–108.

[Hintikka, 2011] Kari A. Hintikka, Tilannekuva.fi. Ehdotus Idea-sarjaan. Kalvoesitys 12.10.2011. Saatavilla: *http://www.slideshare.net/ubiq/apps4finland-2011-ideasarja-tilannekuvafi-kari-a-hintikka-111012-9655310.*

[Hokkanen *et al.*, 2013] Laura Hokkanen, Kari Pylväs, Terhi Kankaanranta, Pekka Paananen, Hanna-Minna Sihvonen ja Hanna Honkavuo, Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa. Osaraportti I - Sosiaalisen median ja älypuhelinsovellusten käyttö viran-

omaisten toiminnassa. Sisäasiainministeriön julkaisu 28/2013, Helsinki, 2013. Saatavilla: *http://www.intermin.fi/julkaisu/282013*

[Hovi, 2009] Christina Hovi, Käytännön kokemukset KERTTU-hankkeesta – Turun ratapiha-alue. Esitys KERTTU-hankkeen loppuseminaarissa 10.6.2009. Saatavilla: *http://www.gaia.fi/files/445/TURKU_HOVI_kaytannon_kokemukset.pdf.*

[Huhtala *et al.*, 2005] Hannele Huhtala, Salli Hakala, Aino Laakso ja Annette Falck, Tiedonkulku ja viestintä Aasian hyökyaaltokatastrofissa. Valtioneuvoston kanslia, Helsinki, 2005.

[Huovila *et al.*, 2010] Henrik Huovila, Jari Korpi, Jari Kortström, Ville Kotovirta, Riitta Molarius, Päivi Mikkonen, Päivi Mäntyniemi, Minna Nissilä, Jenni Rauhala, Tapio Tourula, Nina Wessberg ja Jussi Yliaho. Uhkatilanteiden hallinta. Hälytys-, tilannekuva- ja varoitusjärjestelmän kehittäminen. VTT, 2010.

[HS, 2010] Kehotus pysyä poissa toikin ihmiset bongaamaan karhua. Helsingin Sanomat, 18.6.2010.

[IETF, 2012] Requirements, Terminology and Framework for Exigent Communications. Available at: *http://tools.ietf.org/html/draft-ietf-atoca-requirements-03.*

[ITU-T, 2008] Recommendation X.1303 (09/07): Common alerting protocol (CAP 1.1), ITU-T, 2008. Available at: *http://www.itu.int/rec/T-REC-X.1303-200709-I.*

[JUHTA, 2010] JHS 129 Julkishallinnon verkkopalvelun suunnittelun ja toteuttamisen periaatteet. Julkisen tietohallinnon neuvottelukunta JUHTA, 2010. Saatavilla: *http://docs.jhs-suositukset.fi/jhs-suositukset/JHS129/JHS129.pdf.*

[Järvinen ja Järvinen, 2011] Pertti Järvinen ja Annikki Järvinen, Tutkimustyön metodeista. Opinpajan kirja, 2011.

[Kaján, 2012] Veijo Kaján, VS: Kysymyksiä 25.9. suuronnettomuusharjoituksen Facebook-tiedottamisesta. Vastaanottaja: Mikko Lammi. Lähetetty 5.10.2012. Yksityinen sähköpostiviesti.

[Kauppinen, 2013] Olli Kauppinen, Mobiilipohjaisen hälytysjärjestelmän hyödyntäminen viranomaisviestinnässä ja kriisinhallinnassa: interaktiivinen lähestyminen. Pro gradu -tutkielma, Jyväskylän yliopisto, 2013. Saatavilla: *https://jyx.jyu.fi/dspace/bitstream/handle/123456789/41730/URN%3ANBN%3Afi%3Ajyu-201306111942.pdf.*

[Kazman *et al.*, 2000] Rick Kazman, Mark Klein and Paul Clements. ATAM: Method for architecture evaluation, Carnegie-Mellon University, Technical report CMU/SEI-2000-TR-004, August 2000.

[Kidd *et al.,* 2008] Alisha Kidd, Kevin Loasby, Gavin Treadgold, Kristin Hoskin, Kevin Chong and Scott Caldwell, New Zealand Telecommunications Based Public Alerting Systems Technology Study. Christchurch, New Zealand, New Zealand Centre for Advanced Engineering, University of Canterbury Campus, 2008.

[Kuntaliitto, 2010] Kuntaliitto, Kuntien verkkoviestintäohje. Kuntaliitto, Helsinki, 2010. Saatavilla: *http://www.kunnat.net/fi/asiantuntijapalvelut/viestinta/kuntien-viestinta/kuntaviestinnan-ohjeet/Documents/Verkkoviestintaopas.pdf.*

[Kurtti, 2013] Niko Kurtti, Saatavuuden huomioiminen toteutettaessa web-sovellusta. Diplomityö, Tampereen teknillinen yliopisto, 2013. Saatavilla: *http://URN.fi/URN:NBN:fi:tty-201305171135.*

[Kuula *et al.,* 2013] Jaana Kuula, Vili Auvinen, Olli Kauppinen, Pauli Kettunen, Santtu Viitanen and Tuomo Korhonen, Smartphones as an Alerting, Command and Control. System for the Preparedness Groups and Civilians: Results of Preliminary Tests with the Finnish Police. In: *Proceedings of the 10th International ISCRAM Conference.* Baden-Baden, Germany, 2013, 42-51.

[Laitinen, 2006] Janne Laitinen, GPS-paikkatiedon liittäminen matkapuhelinpalveluihin. Diplomityö, Lappeenrannan teknillinen yliopisto, Lappeenranta, 2006.

[LVM, 2008] Ohje viranomaistiedotteiden lähettämisestä ja hätätiedotteiden välitysjärjestelmän toiminnasta. Liikenne- ja viestintäministeriö, 2008. Saatavilla: *http://www.lvm.fi/web/fi/lomakkeet.*

[LVM, 2009] Julkaisuja 24-2009, VAK-kuljetuskeskittymät osana turvallista yhteiskuntaa – maankäytön suunnittelu ja yhteinen riskienhallinta. KERTTU-hankkeen loppuraportti. Liikenne- ja viestintäministeriö, 2009. Saatavilla: *http://www.lvm.fi/web/fi/julkaisu/-/view/905207.*

[Nurminen *et al.,* 2002] Markku I. Nurminen, Pekka Reijonen ja Jaana Vuorenheimo, Tietojärjestelmän organisatorinen käyttöönotto: kokemuksia ja suuntaviivoja. Turun kaupungin terveystoimen julkaisuja, Sarja A, Nro 1/2002.

[OTK, 2011] Tutkintaselostus S2/2010 Y Heinä-elokuun 2010 rajuilmat. Onnettomuustutkintakeskus, Helsinki, 2011.

[OTK, 2005] Tutkintaselostus A2/2004 Y: Aasian luonnonkatastrofi 26.12.2004. Onnettomuustutkintakeskus, Helsinki, 2005.

[Palttala, 2010] Pipsa Palttala, Kömpelö hätätiedotus halutaan uudistaa. Helsingin Sanomat 15.9.2010.

[Parmes, 2007] Rauli Parmes, *Varautumisen käsikirja*. Tietosanoma Oy, Tallinna 2007.

[Paukkonen, 2005] Matti Paukkonen, Alueellisen käyttäjämäärän seuranta matkaviestinverkossa. Insinöörityö, Savonia-ammattikorkeakoulu, Kuopio 2005.

[Penttinen, 2006a] Jyrki Penttinen, *Tietoliikennetekniikka. Perusverkot ja GSM*. WSOY, Helsinki, 2006.

[Penttinen, 2006b] Jyrki Penttinen, *Tietoliikennetekniikka. 3G ja erityisverkot.* WSOY, Helsinki, 2006.

[Pressman, 2000] Roger S. Pressman, *Software Engineering: A Practitioner's Approach (European Adaptation)*. McGraw-Hill International, London, 2000

[Pylväs *et al.*, 2014] Kari Pylväs, Laura Hokkanen, Pekka Paananen, Terhi Kankaanranta ja Hanna-Minna Sihvonen, Tiedontuotannosta viestintäprosesseihin. Sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa -hanke: osaraportti II. Pelastustopiston julkaisu, B-sarja: Tutkimusraportit 1/2014. Pelastusopisto, Kuopio, 2014.

[Rantala, 2007] Pekka Rantala, *Pelastuslaitoksen onnettomuustiedottamisen perusteet*. Tampere, 2007.

[Razavi, 2011] Sara Modarres Razavi, *Tracking Area Planning in Cellular Networks – Optimization and Performance Evaluation*. Linköping University, Norrköping, 2011. Available at: *http://liu.diva-portal.org/smash/get/diva2:402919/FULLTEXT01.pdf.*

[Räsänen *et al.*, 2005] Teemu Räsänen, Jarkko Tiirikainen, Timo Raatikainen, Matti Paukkonen ja Mikko Kolehmainen. *Matkaviestinoperaattoreiden palvelujärjestelmien hyödyntäminen matkailu- ja ympäristöalan informaatiopalveluissa*. Kuopion yliopisto, Kuopio, 2005.

[Rönkkö, 2008] Teemu Rönkkö, Verkkopaikannukseen perustuvan hätäpaikannukseen haasteet. Pro gradu -tutkielma, Jyväskylän yliopisto, Jyväskylä 2008.

[Seeck *et al.*, 2008] Hannele Seeck, Heidi Lavento ja Salli Hakala, Kriisijohtaminen ja viestintä. Tapaus Nokian vesikriisi. Kuntaliitto, 2008.

[SM, 2010a] Selvitys viranomaistiedotteiden antamisesta. Työryhmän raportti. Sisäasiainministeriö, Helsinki, 2010. Saatavilla: *http://www.intermin.fi/julkaisu/282010?docID=24914*.

[SM, 2010b] Lausuntoyhteenveto. Viranomaistiedotteiden antamista selvittäneen työryhmän raportti. Sisäasiainministeriö, Helsinki, 2010. Saatavilla: *http://www.hare.vn.fi/upload/Asiakirjat/15962/162728_LAUSUNTOYHTEENVETO_VIRANTA-raportista.pdf.*

[SM, 2011] Luonnos hallituksen esitykseksi laiksi vaaratiedotteesta. Lausuntopyyntö. Sisäasiainministeriö, Helsinki, 2011. Saatavilla: *http://www.hare.vn.fi/upload/Asiakirjat/17226/173908_SM007-2011_lausuntopyynt%C3%B6.pdf.*

[SM, 2013] Vaaratiedoteopas. Sisäasiainministeriön julkaisu 1/2013. Saatavilla: *http://www.intermin.fi/julkaisu/012013?docID=39448.*

[SM, 2014] Kohti vuorovaikutteista viranomaisviestintää - sosiaalinen media ja älypuhelinsovellukset kansalaisten avuksi hätätilanteissa - tutkimushankkeen loppuraportti. Sisäministeriö, Helsinki, 2014. Saatavilla: *http://www.intermin.fi/julkaisu/052014*

[Starbird *et al.*, 2013] Kate Starbird, Jim Maddock, Mania Orand, Peg Achterman and Robert M. Mason, Rumors, Flase Flags and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing. University of Washington & Northwest University, 2013. Available at: *http://faculty.washington.edu/kstarbi/Starbird_iConference2014-final.pdf.*

[Tavis & Fitzsimons, 2012] Matt Tavis and Philip Fitzsimons, Amazon Web Services - Web Application Hosting in the AWS Cloud: Best Practices. Amazon Web Services, Inc., 2013. Available at: *http://aws.amazon.com/whitepapers/web-application-hosting-best-practices/.*

[Tilastokeskus, 2013] Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö. Tilastokeskus, Helsinki, 2013. Saatavilla: *http://www.stat.fi/til/sutivi/index.html.*

[TS, 2012] Hätätiedotteet hidastumassa käännöstyön vuoksi. Turun Sanomat 19.10.2012. Saatavilla: *http://www.ts.fi/uutiset/kotimaa/403779/Hatatiedotteet+hidastumassa+kaannostyon+vuoksi.*

[Vanhala, 2011] Lauri Vanhala, Poliisi: Uusiakaan verkkosivuja ei mitoiteta kestämään kävijäpiikkejä. Suomen Kuvalehti, 9.11.2011. Saatavilla *http://suomenkuvalehti.fi/jutut/kotimaa/poliisi-uusiakaan-verkkosivuja-ei-mitoiteta-kestamaan-kavijapiikkeja.*

[Viestintävirasto, 2004] Työryhmäraportti 2/2004, Viestintäverkkojen tekniset viranomaisvaatimukset. Hätäpuhelupaikannuksen tekninen ratkaisu Suomessa. Viestintävirasto, Helsinki, 2004. Saatavilla *http://www.ficora.fi/attachments/suomiry/1156442801620/TRaportti022004.pdf*.

[Viestintävirasto, 2005] Työryhmäraportti 7/2005, Tekstiviestijärjestelmät väestön varoittamisessa. Viestintävirasto, Helsinki, 2005.

[Vieveg *et al.*, 2010] Sarah Vieveg, Amanda L. Hughes, Kate Starbird and Leysia Plaen, Microblogging During Two Natural Hazards Events: What Twitter May Contribute to Situational Awareness. In: *Proceedings of the*

28thIinternational ACM Conference on Human Factors in Computer Systems (2010), ACM, 1079-1088.

[VIRVA, 2009] Ehdotus kohdennettujen viranomaistiedotteiden käyttöönotosta väestön hälyttämisen ja varoituksen tukena. Viranomaistiedotuksen varmistusryhmä VIRVA (Liikenne- ja viestintäministeriö), Helsinki, 2009. Saatavilla: *http://www.lvm.fi/web/fi/tiedote/-/view/907447.*

[VTT, 2009] Suomen eCall-verkkosivut. http://www.ecall.fi. Viitattu 23.10.2012.

[Wiio, 2013] Osmo A. Wiio, Wiion lait. Saatavilla: *http://osmo.wiio.net/wiion-lait/* (Viitattu: 28.10.2013).

[Wong, 2013] Karen Wong, E9-1-1 Phase II Location Accuracy, State of California. California Governor's Office of Emergency Services. Available at: *http://transition.fcc.gov/bureaus/pshs/911/Phase%202/Workshop_11_2013/California_911_Wong_Nov2013.pdf.*

[Woodcock, 2009] Jody Woodcock, Leveraging Social Media to Engage the Public in Homeland Security. Master's Thesis, Naval Postgraduation School, Monterey, 2009. Available at: *http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA509065&Location=U2&doc=GetTRDoc.pdf.*

[Yamazaki, 2012] Erika Yamasaki, What we can learn from Japan's Early Earthquake Warning System. Momentum, 1, 2012. Available at: *https://sites.sas.upenn.edu/momentum/files/yamasaki.pdf.*

[YLE, 2009] Kännykkäpaikannus siirtyi nettiin. YLE Uutiset, 26.5.2009. Saatavilla: *http://yle.fi/uutiset/kannykkapaikannus_siirtyi_nettiin/5256132.*

[YLE, 2013] Uudet vaaratiedotteet hämmentävät ja ärsyttävät – määrä yllätti myös viranomaiset. YLE Uutiset, 28.6.2013. Saatavilla: *http://yle.fi/uutiset/uudet_vaaratiedotteet_hammentavat_ja_arsyttavat_-_maara_yllatti_myos_viranomaiset/6709779.*

Liite 1. Esimerkki CAP-muotoisesta hätäsanomasta

Esimerkkiviesti ITU-T:n suosituksen X.1303 [ITU-T, 2008] mukaisesta Common alerting protocol (CAP 1.1) –muodossa esitetystä sanomasta XML-notaationa.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
     <identifier>KSTO1055887203</identifier>
     <sender>KSTO@NWS.NOAA.GOV</sender>
     <sent>2003-06-17T14:57:00-07:00</sent>
     <status>Actual</status>
     <msgType>Alert</msgType>
     <scope>Public</scope>
     <info>
          <category>Met</category>
          <event>SEVERE THUNDERSTORM</event>
          <responseType>Shelter</responseType>
          <urgency>Immediate</urgency>
          <severity>Severe</severity>
          <certainty>Observed</certainty>
          <eventCode>
               <valueName>same</valueName>
               <value>SVR</value>
          </eventCode>
          <expires>2003-06-17T16:00:00-07:00</expires>
          <senderName>NATIONAL WEATHER SERVICE SACRAMENTO
          CA</senderName>
          <headline>SEVERE THUNDERSTORM WARNING</headline>
          <description> AT 254 PM PDT...NATIONAL WEATHER SERVICE
          DOPPLER RADAR INDICATED
          A SEVERE THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY...OR
          ABOUT 18 MILES
          SOUTHEAST OF KIRKWOOD...MOVING
          SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND STRONG DAMAGING
          WINDS ARE LIKELY
          WITH THIS STORM.</description>
          <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE
          STORM
          PASSES.</instruction>
          <contact>BARUFFALDI/JUSKIE</contact>
          <area>
               <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN
               CALIFORNIA, EXTREME
               NORTHEASTERN CALAVERAS COUNTY IN CALIFORNIA,
               SOUTHWESTERN ALPINE COUNTY IN
               CALIFORNIA</areaDesc>
               <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74
               38.62,-119.89 38.47,-
               120.14</polygon>
               <geocode>
                    <valueName>FIPS6</valueName>
                    <value>006109</value>
               </geocode>
               <geocode>
                    <valueName>FIPS6</valueName>
                    <value>006009</value>
               </geocode>
               <geocode>
                    <valueName>FIPS6</valueName>
                    <value>006003</value>
               </geocode>
          </area>
     </info>
</alert>
```